Proteja las cargas de trabajo

BlueXP ransomware protection

NetApp
October 07, 2024

Tabla de contenidos

Proteja las cargas de trabajo

Proteger cargas de trabajo con estrategias de ransomware

Puedes proteger las cargas de trabajo contra ataques de ransomware completando las siguientes acciones mediante la protección contra ransomware de BlueXP.

- Habilite la protección coherente con las cargas de trabajo, que funciona con el software SnapCenter o el complemento SnapCenter para VMware vSphere.
- Cree o gestione estrategias de protección frente al ransomware, que incluyen políticas que cree para copias Snapshot, backups y protección frente al ransomware (conocidas como *políticas de detección*).
- Importe una estrategia y ajústela.
- Agrupe los recursos compartidos de archivos para que le resulte más fácil proteger las cargas de trabajo en lugar de protegerlas individualmente.
- Elimina una estrategia de protección contra ransomware.

*¿Qué servicios se utilizan en la protección? * Los siguientes servicios pueden utilizarse para gestionar las políticas de protección. La información sobre protección de estos servicios aparece en la protección contra ransomware de BlueXP :

- Backup y recuperación de BlueXP para recursos compartidos de archivos y recursos compartidos de archivos de equipos virtuales
- SnapCenter para VMware para almacenes de datos de máquinas virtuales
- SnapCenter para Oracle y MySQL

Políticas de protección

Puede resultar útil revisar información sobre las políticas de protección que se pueden cambiar y qué tipos de políticas existen en una estrategia de protección.

¿Qué políticas de protección puedes cambiar?

Puede cambiar las políticas de protección en función de la protección de las cargas de trabajo que tenga:

- **Las cargas de trabajo no están protegidas por aplicaciones NetApp**: Estas cargas de trabajo no están gestionadas por SnapCenter, el complemento SnapCenter para VMware vSphere o la copia de seguridad y recuperación de BlueXP . Estas cargas de trabajo pueden tener copias Snapshot realizadas como parte de ONTAP u otros productos. Si existe protección de ONTAP FPolicy, puede cambiar la protección de FPolicy mediante ONTAP.
- **Cargas de trabajo con protección existente de aplicaciones NetApp**: Estas cargas de trabajo tienen políticas de copias de seguridad o instantáneas administradas por SnapCenter, SnapCenter para VMware vSphere o copias de seguridad y recuperación de BlueXP .
  - Si SnapCenter, SnapCenter para VMware o el sistema de backup y recuperación de datos de BlueXP gestionan las políticas de backup o Snapshot, seguirán siendo gestionadas por estas aplicaciones. Con la protección frente al ransomware de BlueXP , también puedes aplicar una política de detección de ransomware a esas cargas de trabajo.
  - Si la protección autónoma de ransomware (ARP) y FPolicy en ONTAP gestionan una política de detección de ransomware, esas cargas de trabajo estarán protegidas y seguirán gestionándolas por

ARP y FPolicy.

*¿Qué políticas se requieren en una estrategia de protección contra ransomware? *

Las siguientes políticas son necesarias en la estrategia de protección contra ransomware:

- Política de detección de ransomware
- Política de Snapshot

No es necesaria una política de backup en la estrategia de protección frente a ransomware de BlueXP .

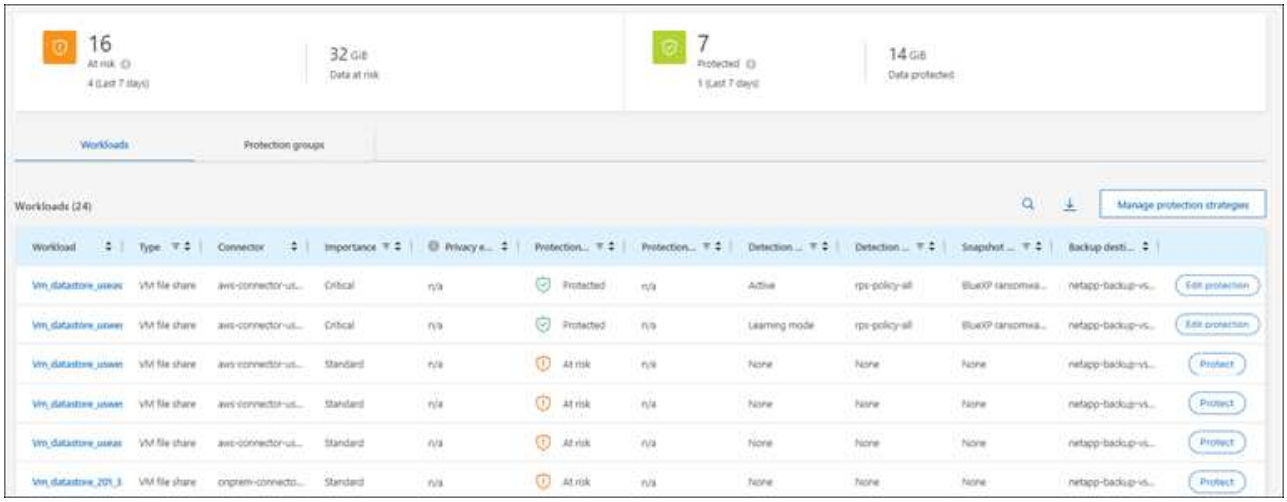
Mira la protección contra ransomware en una carga de trabajo

Uno de los primeros pasos para proteger las cargas de trabajo es visualizar las cargas de trabajo actuales y su estado de protección. Se pueden ver los siguientes tipos de cargas de trabajo:

- Cargas de trabajo de aplicaciones
- Cargas de trabajo de máquinas virtuales
- Cargas de trabajo de recursos compartidos de archivos

Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección** > **Protección contra ransomware**.
2. Debe realizar una de las siguientes acciones:
   - En el panel Protección de datos del panel, seleccione **Ver todo**.
   - En el menú, selecciona **Protección**.



3. En esta página, puede ver y cambiar los detalles de protección de la carga de trabajo.

> Para las cargas de trabajo que ya poseen una política de protección con un servicio de backup y recuperación de datos de SnapCenter o BlueXP, no se puede editar la protección. Para estas cargas de trabajo, el ransomware de BlueXP permite la protección autónoma frente a ransomware o la protección de FPolicy si ya están activados en otros servicios. Más información sobre "Protección autónoma de ransomware", "Backup y recuperación de BlueXP"y "FPolicy de ONTAP".

Detalles de protección en la página Protection

En la página Protection, se muestra la siguiente información sobre la protección de cargas de trabajo:

Estado de protección: Una carga de trabajo puede mostrar uno de los siguientes estados de protección para indicar si se aplica o no una política:

- **Protegido**: Se aplica una política. ARP está habilitado en todos los volúmenes relacionados con la carga de trabajo.
- **En riesgo**: No se aplica ninguna política. Si una carga de trabajo no tiene activada una política de detección primaria, está «en riesgo» aunque tenga activada una política de instantáneas y de backup.
- **En progreso**: Se está aplicando una política pero aún no se ha completado.
- **Fallo**: Se aplica una política pero no funciona.

Estado de detección: Una carga de trabajo puede tener uno de los siguientes estados de detección de ransomware:

- **Aprendizaje**: Recientemente se asignó una política de detección de ransomware a la carga de trabajo y el servicio está escaneando cargas de trabajo.
- **Activo**: Se asigna una política de protección de detección de ransomware.
- **No establecido**: No se asigna una política de protección de detección de ransomware.
- **Error**: Se asignó una política de detección de ransomware, pero el servicio encontró un error.

Cuando se habilita la protección en la protección frente a ransomware de BlueXP , la detección de alertas y la generación de informes se inician después de que el estado de la política de detección de ransomware cambie del modo de aprendizaje al modo activo.

Política de detección: Aparece el nombre de la política de detección de ransomware, si se ha asignado una. Si la política de detección no se ha asignado, aparece N/A.

Políticas de instantáneas y copias de seguridad: Esta columna muestra las políticas de instantáneas y copias de seguridad aplicadas a la carga de trabajo y al producto o servicio que administra dichas políticas.

- Gestionado por SnapCenter
- Gestionado por el plugin de SnapCenter para VMware vSphere
- Gestionado por backup y recuperación de datos de BlueXP
- Nombre de la política de protección contra ransomware que rige las copias Snapshot y los backups
- Ninguno

Importancia de la carga de trabajo

La protección frente al ransomware de BlueXP asigna una importancia o prioridad a cada carga de trabajo durante la detección, en función de un análisis de cada carga de trabajo. La importancia de la carga de trabajo se determina en las siguientes frecuencias de snapshots:

- **Crítico**: Copias instantáneas tomadas más de 1 por hora (programa de protección altamente agresivo)
- **Importante**: Copias instantáneas tomadas menos de 1 por hora pero más de 1 por día
- **Estándar**: Copias instantáneas tomadas más de 1 por día

Políticas de detección predefinidas

Puedes elegir una de las siguientes políticas predefinidas de protección contra ransomware de BlueXP , que están alineadas con la importancia de la carga de trabajo:

Nivel de política	Snapshot	Frecuencia	Retención (días)	n.o de copias snapshot	Número máximo total de copias Snapshot
Política de carga de trabajo crítica	Cada trimestre	Cada 15 min	3	288	309
	Todos los días	Cada 1 días	14	14	309
	Semanal	Cada 1 semanas	35	5	309
	Mensual	Cada 30 días	60	2	309
Política de carga de trabajo importante	Cada trimestre	Cada 30 minutos	3	144	165
	Todos los días	Cada 1 días	14	14	165
	Semanal	Cada 1 semanas	35	5	165
	Mensual	Cada 30 días	60	2	165
Política de carga de trabajo estándar	Cada trimestre	Cada 30 min	3	72	93
	Todos los días	Cada 1 días	14	14	93
	Semanal	Cada 1 semanas	35	5	93
	Mensual	Cada 30 días	60	2	93

Habilite una protección coherente con las aplicaciones o las máquinas virtuales con SnapCenter

La habilitación de la protección coherente con la aplicación o las máquinas virtuales ayuda a proteger las cargas de trabajo de sus aplicaciones o máquinas virtuales de una forma coherente, lo que consigue un estado inactivo y consistente para evitar la pérdida potencial de datos posteriormente si es necesario la recuperación.

Este proceso inicia el registro del servidor de software de SnapCenter para aplicaciones o el plugin de SnapCenter para VMware vSphere para máquinas virtuales mediante el backup y la recuperación de BlueXP.

Después de habilitar la protección consistente con la carga de trabajo, podrás gestionar las estrategias de protección en la protección frente al ransomware de BlueXP. La estrategia de protección incluye la instantánea y las políticas de backup gestionadas en otras partes, junto con una política de detección de ransomware gestionada en la protección frente al ransomware de BlueXP .

Para obtener más información sobre el registro de SnapCenter o el plugin de SnapCenter para VMware vSphere mediante el backup y la recuperación de BlueXP, consulte la siguiente información:

- "Registre el software del servidor SnapCenter"
- "Registre el plugin de SnapCenter para VMware vSphere"

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Dashboard**.
2. En el panel Recomendaciones, busque una de las siguientes recomendaciones y seleccione **Revisar y corregir**:
   - Regístrate Servidor SnapCenter disponible con BlueXP
   - Registre el plugin de SnapCenter para VMware vSphere (SCV) con BlueXP
3. Siga la información para registrar el host de SnapCenter o el plugin de SnapCenter para VMware vSphere con el backup y la recuperación de BlueXP.
4. Vuelve a la protección contra el ransomware de BlueXP.
5. En la protección contra ransomware de BlueXP, accede a la consola e inicia de nuevo el proceso de detección.
6. En Protección contra ransomware de BlueXP, selecciona **Protección** para ver la página Protección.
7. Revise los detalles de la columna Snapshot y backup policies de la página Protection para ver que las políticas se gestionan en otros lugares.

Añada una estrategia de protección contra ransomware

Puedes añadir una estrategia de protección contra ransomware a las cargas de trabajo. La forma de hacerlo depende de si ya existen políticas de Snapshot y backup:

- * Cree una estrategia de protección contra ransomware si no tiene instantáneas o políticas de copia de seguridad*. Si las copias Snapshot o las políticas de backup no existen en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que crea en la protección contra ransomware de BlueXP :
  - Política de Snapshot
  - Política de backup
  - Política de detección de ransomware
- **Crear una política de detección para cargas de trabajo que ya tienen políticas de instantáneas y copias de seguridad**, que se administran en otros productos o servicios de NetApp. La política de detección no cambiará las políticas gestionadas en otros productos.

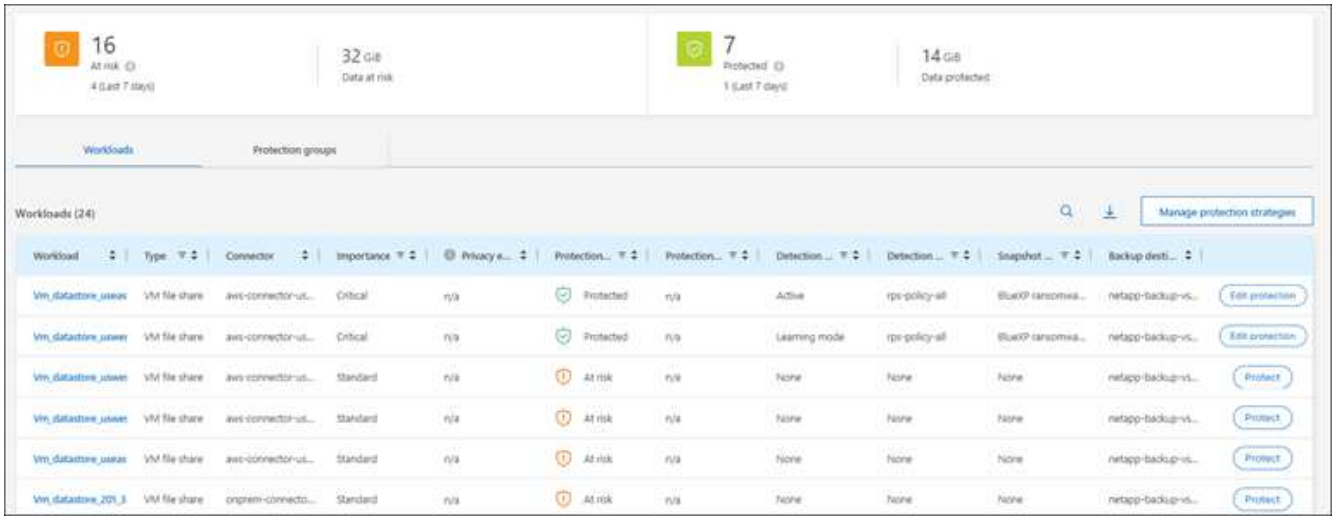
Crear una estrategia de protección contra ransomware (si no tiene snapshots ni políticas de backup)

Si las copias Snapshot o las políticas de backup no existen en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que crea en la protección contra ransomware de BlueXP :

- Política de Snapshot
- política de backup
- Política de detección de ransomware

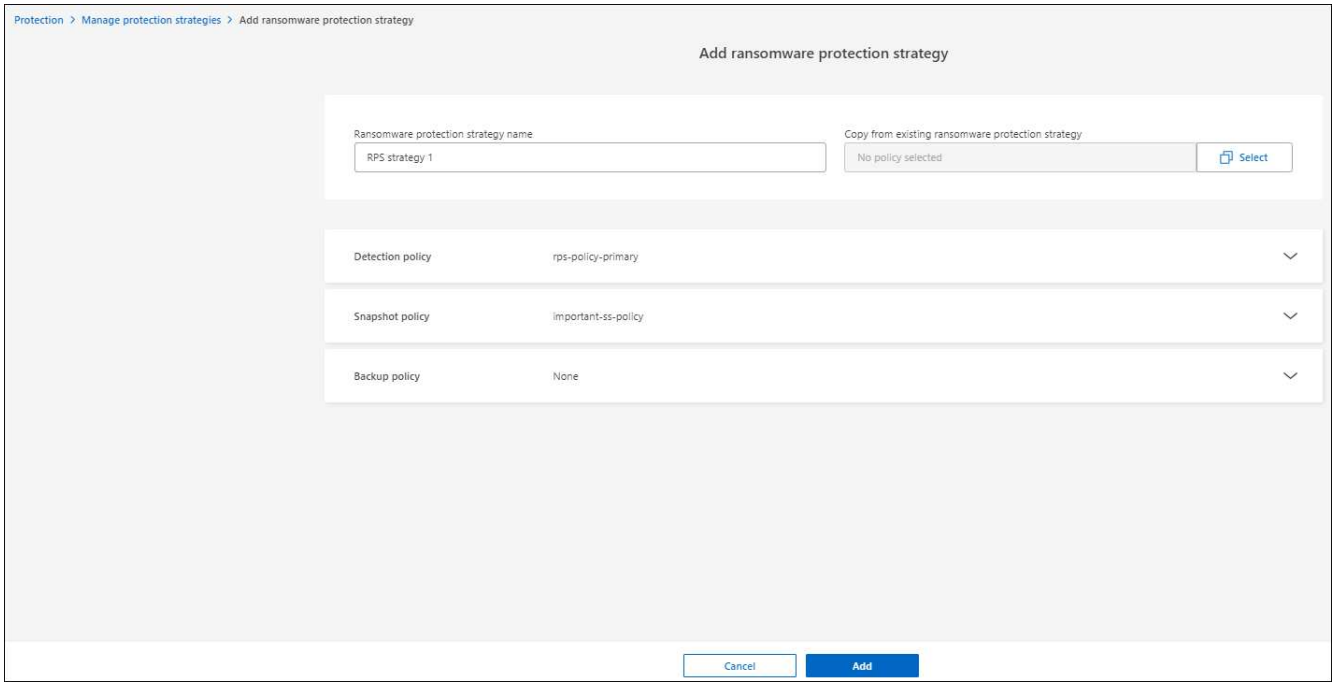
Pasos para crear una estrategia de protección contra el ransomware

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.



2. En la página Protección, selecciona **Administrar estrategias de protección**.

3. En la página Estrategias de protección contra ransomware, selecciona **Agregar**.



4. Introduzca un nuevo nombre de estrategia o introduzca un nombre existente para copiarlo. Si introduce un nombre existente, elija el que desea copiar y seleccione **Copiar**.

   Si decide copiar y modificar una estrategia existente, el servicio agrega «_copy» al nombre original. Debe cambiar el nombre y al menos una configuración para que sea única.

5. Para cada elemento, seleccione la flecha **abajo**.

   - **Política de detección**:
     - **Política**: Elija una de las políticas de detección prediseñadas.
     - **Detección primaria**: Habilita la detección de ransomware para que el servicio detecte posibles ataques de ransomware.
     - **Extensiones de archivo de bloque**: Permite que este tenga el bloqueo de servicio conocido extensiones de archivo sospechosas. El servicio realiza copias Snapshot automatizadas cuando la detección primaria está habilitada.

       Si desea cambiar las extensiones de archivo bloqueadas, edítelas en System Manager.
   - **Política de Snapshot**:
     - **Nombre base de la política de instantáneas**: Seleccione una política o seleccione **Crear** e introduzca un nombre para la política de instantáneas.
     - **Bloqueo de instantáneas**: Permite que esto bloquee las copias instantáneas en el almacenamiento primario para que no se puedan modificar o eliminar durante un cierto período de tiempo, incluso si un ataque de ransomware se dirige al destino de almacenamiento de la copia de seguridad. Esto también se denomina *almacenamiento inmutable*. Esto permite acelerar el tiempo de restauración.

       Cuando una snapshot está bloqueada, la hora de caducidad del volumen se establece en la hora de caducidad de la copia Snapshot.

     ONTAP 9.12.1 y las versiones posteriores ofrecen el bloqueo de copias de SnapVault. Para obtener más información acerca de SnapLock, consulte "SnapLock en ONTAP".

     - **Programaciones de instantáneas**: Elija las opciones de programación, el número de copias de instantáneas que desea conservar y seleccione habilitar la programación.
   - **Política de respaldo**:
     - **Backup policy basename**: Introduce un nombre nuevo o elige un nombre existente.
     - **Horarios de copia de seguridad**: Elija opciones de programación para el almacenamiento secundario y habilite el horario.

   Para habilitar el bloqueo de copia de seguridad en el almacenamiento secundario, configure sus destinos de copia de seguridad usando la opción **Settings**. Para obtener más información, consulte "Configurar ajustes".

6. Seleccione **Agregar**.

Añada una política de detección a las cargas de trabajo que ya tengan políticas de Snapshot y backup

Con la protección frente a ransomware de BlueXP , puedes asignar una política de detección de ransomware a cargas de trabajo que ya tengan políticas de backup y Snapshot que se gestionen en otros productos o

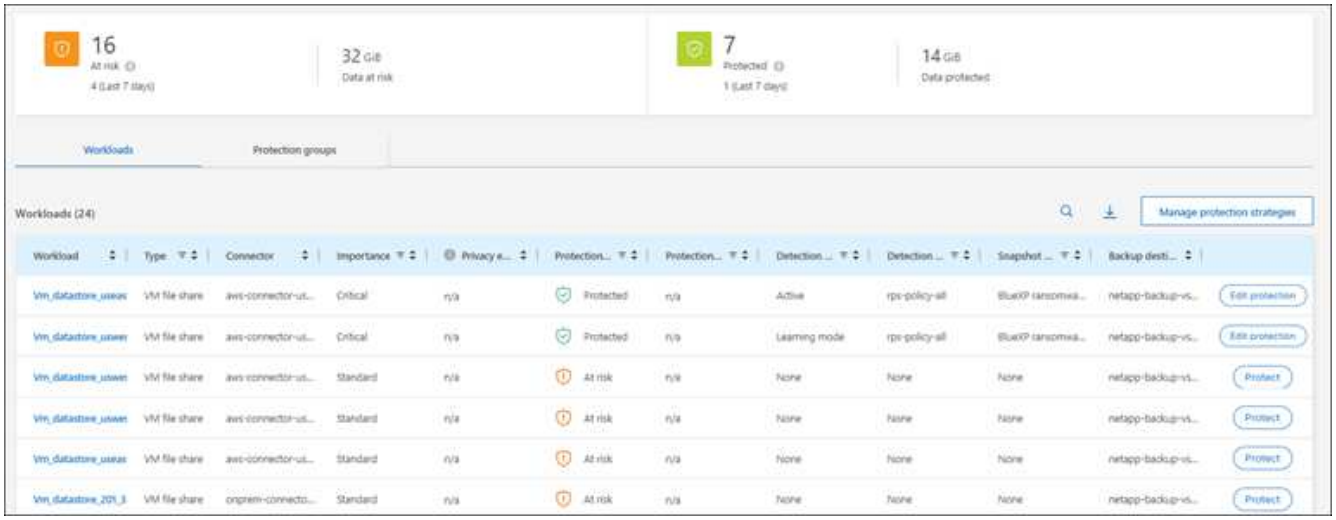
servicios de NetApp. La política de detección no cambiará las políticas gestionadas en otros productos.

Otros servicios, como el backup y recuperación de BlueXP y SnapCenter, usan los siguientes tipos de políticas para gobernar las cargas de trabajo:

- Políticas que rigen las snapshots
- Normativas que rigen la replicación en el almacenamiento secundario
- Directivas que rigen los backups del almacenamiento de objetos

Pasos

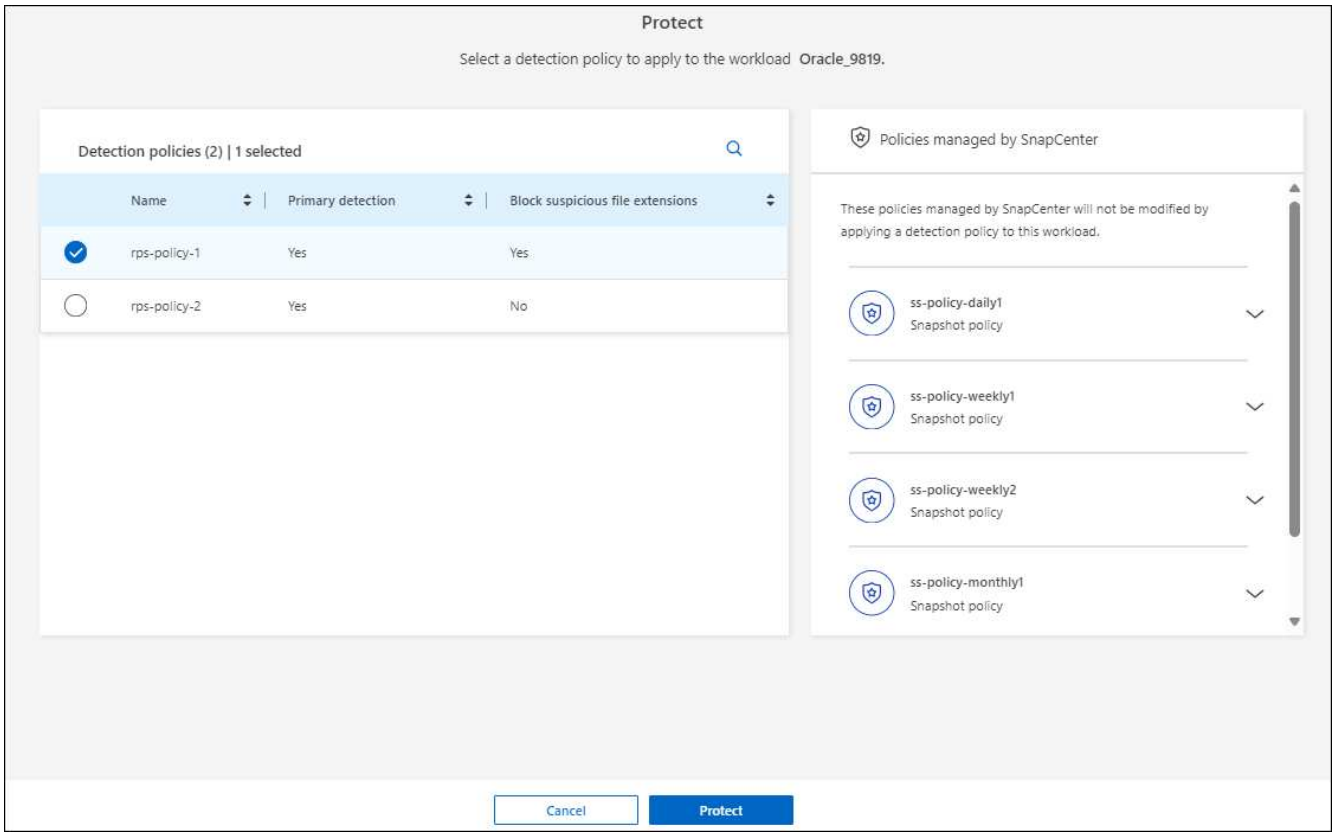
1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.



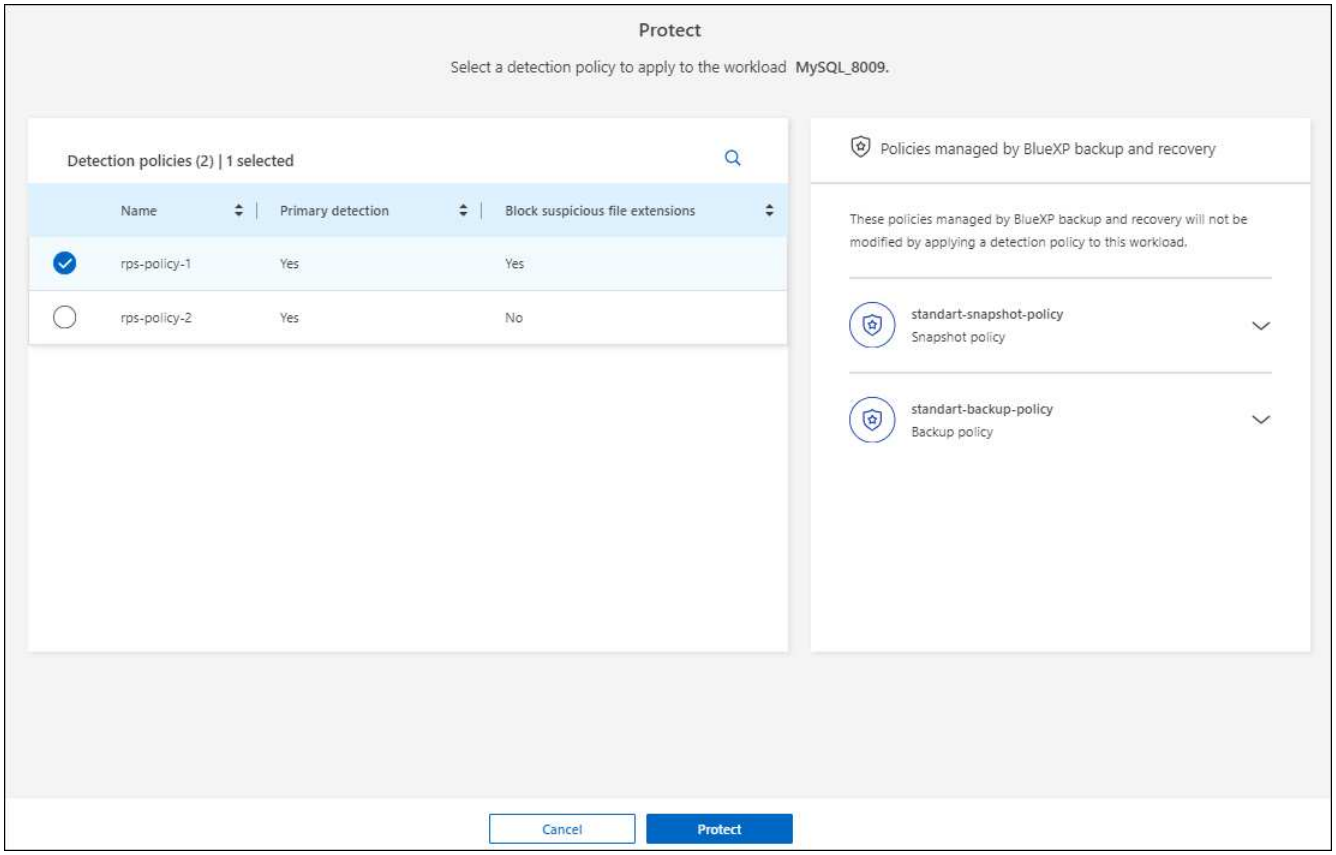
2. En la página Protección, seleccione una carga de trabajo y seleccione **Proteger**.

   La página Protect muestra las políticas gestionadas por el software de SnapCenter, SnapCenter para VMware vSphere y backup y recuperación de BlueXP.

   El siguiente ejemplo muestra las políticas gestionadas por SnapCenter:



En el siguiente ejemplo se muestran las políticas gestionadas por backup y recuperación de datos de BlueXP:



3. Para ver los detalles de las políticas administradas en otro lugar, haga clic en la flecha **abajo**.
4. Para aplicar una política de detección además de las políticas de instantáneas y copias de seguridad gestionadas en otros lugares, seleccione la política de detección.
5. Seleccione **Proteger**.
6. En la página Protección, revise la columna Política de detección para ver la política de detección asignada. Además, la columna Instantánea y políticas de copia de seguridad muestra el nombre del producto o servicio que gestiona las políticas.

Asigne una política diferente

Puede asignar una política de protección diferente a la actual.

Pasos

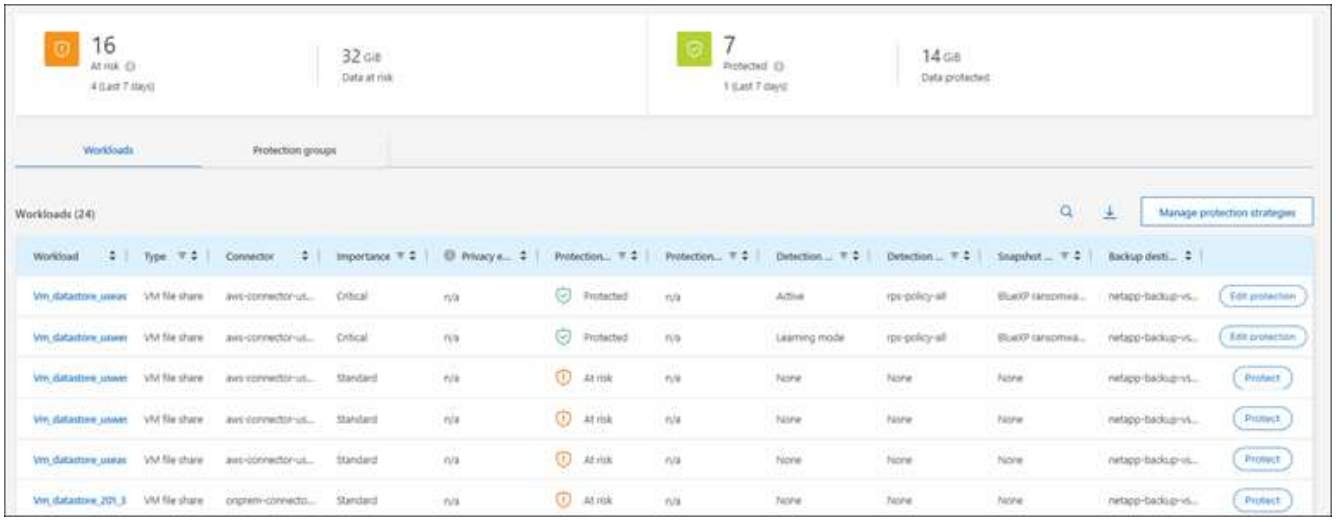
1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, en la fila de carga de trabajo, seleccione **Editar protección**.
3. En la página Policies, haga clic en la flecha hacia abajo de la política que desea asignar para revisar los detalles.
4. Seleccione la política que desea asignar.
5. Selecciona **Proteger** para finalizar el cambio.

Agrupe los recursos compartidos de archivos para una protección más sencilla

La agrupación de recursos compartidos de archivos facilita la protección del patrimonio de datos. El servicio puede proteger todos los volúmenes de un grupo a la vez, en lugar de proteger cada volumen por separado.

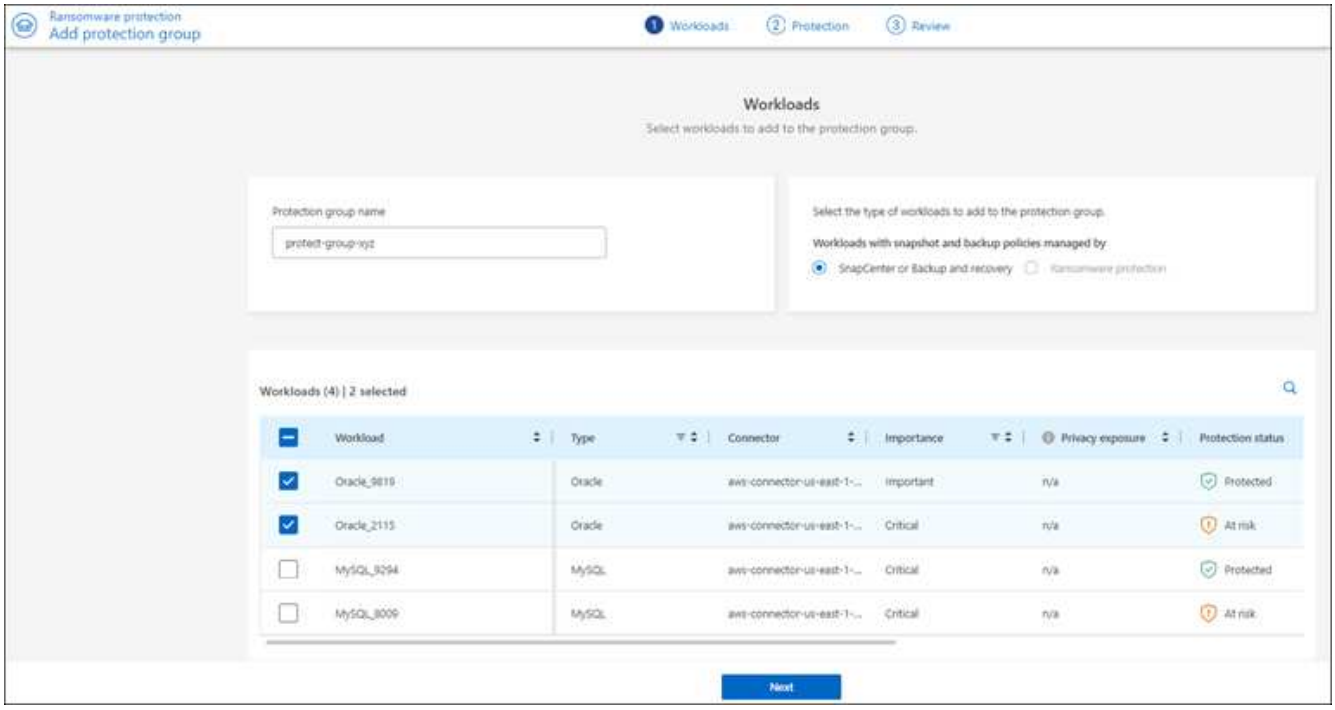
Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.



2. En la página Protección, seleccione la pestaña **Grupos de protección**.

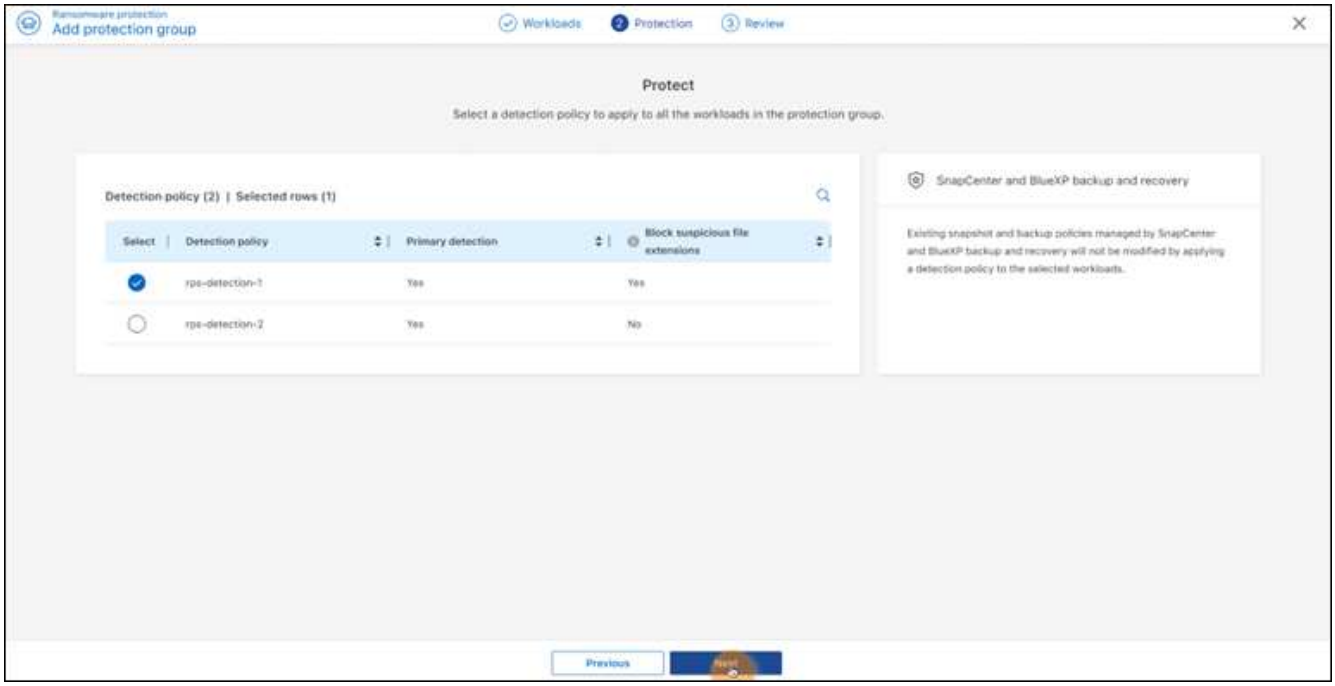
3. Seleccione **Agregar**.



4. Introduzca un nombre para el grupo de protección.
5. Realice uno de los siguientes pasos:
   a. Si ya cuenta con políticas de protección, seleccione si desea agrupar cargas de trabajo según si las gestiona una de estas:
      - Protección contra ransomware de BlueXP
      - Backup y recuperación de datos de SnapCenter o BlueXP
   b. Si ya no tienes políticas de protección implementadas, la página muestra las estrategias preconfiguradas de protección contra ransomware.
      i. Elige uno para proteger tu grupo y selecciona **Siguiente**.
      ii. Si la carga de trabajo que ha elegido tiene volúmenes en varios entornos de trabajo, seleccione el destino de backup para los múltiples entornos de trabajo para que se puedan hacer backups en el cloud.
6. Seleccione las cargas de trabajo que se añadirán al grupo.

Para ver más información sobre las cargas de trabajo, desplácese a la derecha.

7. Seleccione **Siguiente**.



8. Seleccione la política que regirá la protección de este grupo.
9. Seleccione **Siguiente**.
10. Revise las selecciones del grupo de protección.
11. Seleccione **Agregar**.

Añada más cargas de trabajo a un grupo

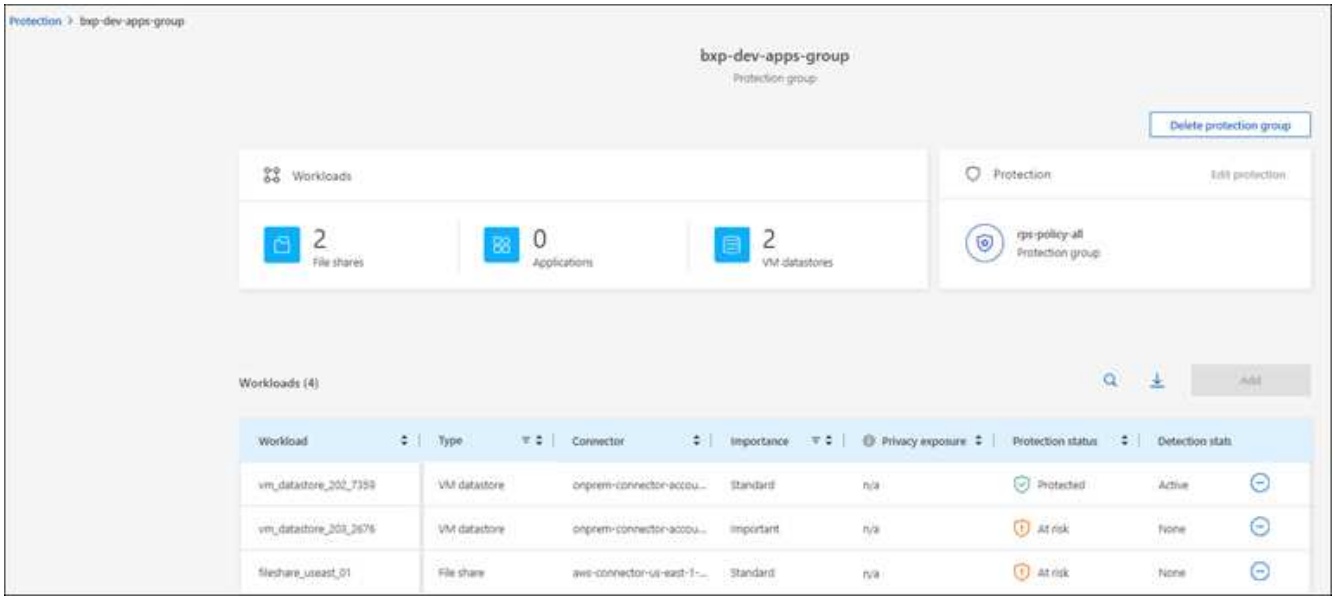
Es posible que más adelante deba agregar más cargas de trabajo a un grupo existente.

Si el grupo incluye cargas de trabajo gestionadas solo mediante la protección contra ransomware de BlueXP (y no mediante el backup y recuperación de datos de SnapCenter o BlueXP), debería usar grupos separados para cargas de trabajo que gestionen solo con la protección contra ransomware de BlueXP y otro grupo para cargas de trabajo gestionadas por otros servicios.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, seleccione la pestaña **Grupos de protección**.

3. Seleccione el grupo al que desea añadir más cargas de trabajo.



4. En la página del grupo de protección seleccionado, seleccione **Agregar**.

   La protección frente a ransomware de BlueXP muestra que solo las cargas de trabajo que no se encuentran en el grupo que usan las mismas políticas de snapshot y backup que el grupo.

   La parte superior de la página muestra qué servicio mantiene las políticas de instantánea, copia de seguridad y detección.

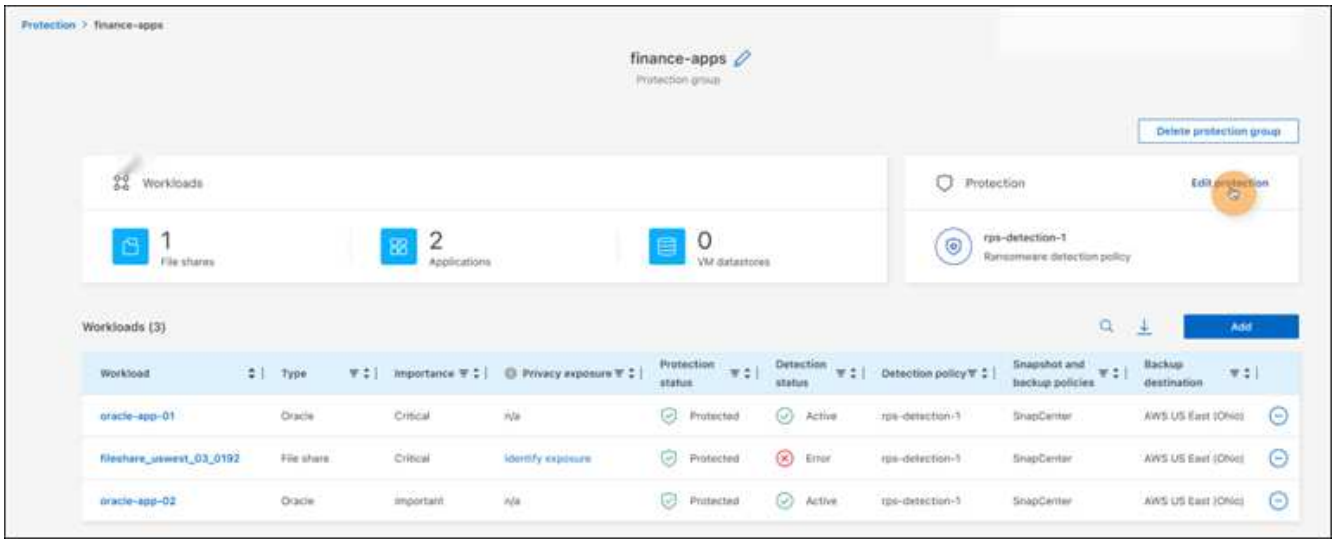
5. Seleccione las cargas de trabajo adicionales que se deben añadir al grupo.
6. Seleccione **Guardar**.

Editar protección de grupo

Puede cambiar la política de detección en un grupo existente. Si la política de detección aún no se ha agregado a este grupo, puede agregarla ahora.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, seleccione la pestaña **Grupos de protección**.



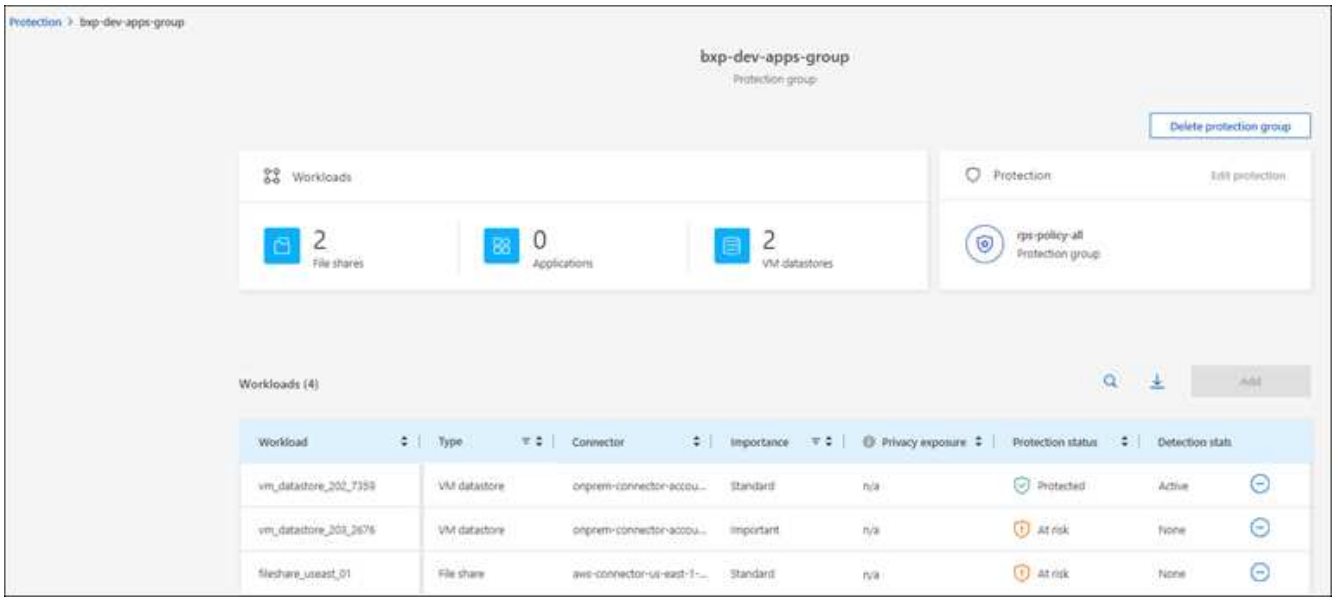
3. En el panel Protección, seleccione **Editar protección**.
4. Seleccione o agregue una política de detección a este grupo.

Quitar cargas de trabajo de un grupo

Es posible que más adelante deba eliminar cargas de trabajo de un grupo existente.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del que desea quitar una o varias cargas de trabajo.



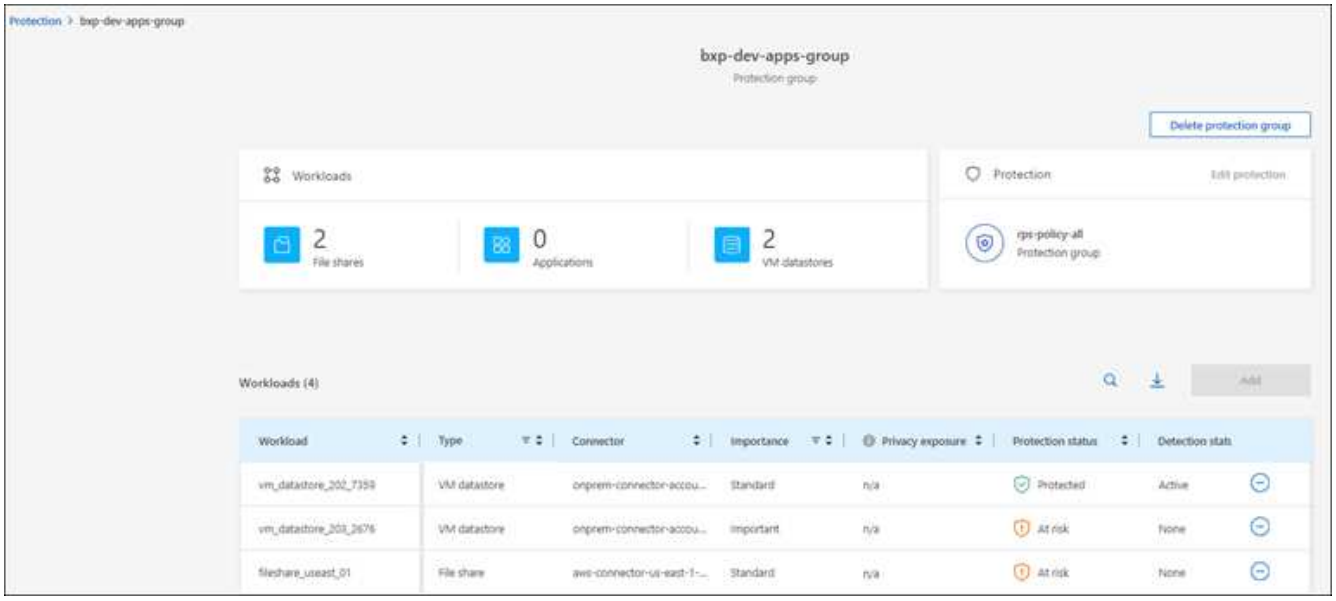
4. En la página del grupo de protección seleccionado, seleccione la carga de trabajo que desea eliminar del grupo y seleccione la opción *Acciones*•••.
5. En el menú Acciones, seleccione **Eliminar carga de trabajo**.
6. Confirme que desea eliminar la carga de trabajo y seleccione **Eliminar**.

Elimine el grupo de protección

Al eliminar el grupo de protección se quita el grupo y su protección, pero no se quitan las cargas de trabajo individuales.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del que desea quitar una o varias cargas de trabajo.



4. En la página del grupo de protección seleccionado, en la parte superior derecha, selecciona **Eliminar grupo de protección**.
5. Confirme que desea eliminar el grupo y seleccione **Eliminar**.

Gestionar las estrategias de protección frente al ransomware

Puedes eliminar una estrategia de ransomware.

Mira cargas de trabajo protegidas por una estrategia de protección frente al ransomware

Antes de eliminar una estrategia de protección contra ransomware, es posible que desee ver qué cargas de trabajo están protegidas por esa estrategia.

Puede ver las cargas de trabajo desde la lista de estrategias o cuando está editando una estrategia específica.

Pasos para ver la lista de estrategias

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, selecciona **Administrar estrategias de protección**.

   La página Estrategias de protección contra ransomware muestra una lista de estrategias.

3. En la página Ransomware protection Strategies, en la columna Protected Workloads, haga clic en la flecha hacia abajo al final de la fila.

Elimina una estrategia de protección contra ransomware

Es posible eliminar una estrategia de protección que actualmente no esté asociada a ninguna carga de trabajo.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
2. En la página Protección, selecciona **Administrar estrategias de protección**.
3. En la página Administrar estrategias, selecciona la opción **Acciones** ••• para la estrategia que deseas eliminar.
4. En el menú Acciones, selecciona **Eliminar política**.