Proteger las cargas de trabajo

NetApp Ransomware Resilience

NetApp
February 19, 2026

Tabla de contenidos

Proteger las cargas de trabajo . . . 1
Revisa el estado de la protección en NetApp Ransomware Resilience . . . 1
Ver la protección en una carga de trabajo . . . 1
Entiende el panel de control de protección . . . 2
Próximos pasos . . . 3
Proteja las cargas de trabajo con las estrategias de protección NetApp Ransomware Resilience . . . 3
Comprender las estrategias de protección contra ransomware . . . 3
Agregar una estrategia de protección contra ransomware . . . 6
Gestionar estrategias de protección contra ransomware . . . 11
Administra los grupos de protección en NetApp Ransomware Resilience . . . 12
Crear un grupo de protección . . . 12
Eliminar cargas de trabajo de un grupo de protección . . . 15
Eliminar un grupo de protección . . . 15
Busque información de identificación personal con la NetApp Data Classification en Ransomware Resilience . . . 16
Identificar la exposición a la privacidad con la clasificación de datos . . . 16
Revisar la exposición a la privacidad . . . 17
El impacto de la exposición a la privacidad en la importancia de la carga de trabajo . . . 18
Para más información . . . 19

Proteger las cargas de trabajo

Revisa el estado de la protección en NetApp Ransomware Resilience

El panel de protección de NetApp Ransomware Resilience te da una visión general del estado de protección y la preparación de tus cargas de trabajo. Usa el panel de protección para ver qué está protegido, qué necesita protección y cuál es el alcance de la protección.

Una vez que entiendas el alcance de tu protección actual, "puedes crear y aplicar estrategias de protección contra ransomware a tus cargas de trabajo".

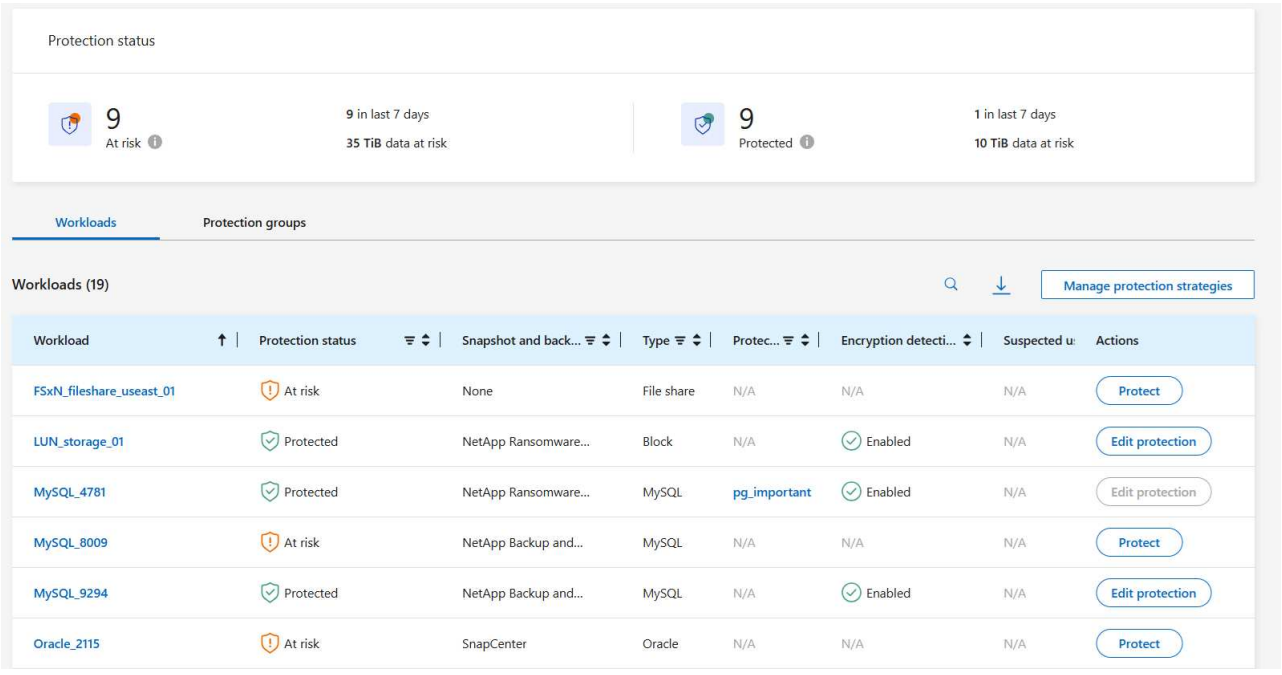
Ver la protección en una carga de trabajo

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

- Cargas de trabajo de aplicaciones
- Bloquear cargas de trabajo
- Cargas de trabajo de uso compartido de archivos
- Cargas de trabajo de máquinas virtuales

Pasos

1. Desde la navegación izquierda de la consola, seleccione **Protección** > **Resiliencia ante ransomware**.
2. Debe realizar una de las siguientes acciones:
   - Desde el panel de Protección de datos en el Tablero, seleccione **Ver todo**.
   - Desde el menú, seleccione **Protección**.



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

> Consulta "Agregar una estrategia de protección contra ransomware" para aprender sobre el uso de Ransomware Resilience cuando ya hay una política de protección con Backup and Recovery.

Entiende el panel de control de protección

El panel de protección en Ransomware Resilience muestra información detallada sobre las cargas de trabajo (por ejemplo, nombre y tipo de carga de trabajo, agente de Console, sistema y máquina virtual de almacenamiento), además de información sobre el estado de la protección. Usa el panel de protección para revisar y gestionar la preparación frente al ransomware de las cargas de trabajo. Las siguientes columnas son especialmente útiles para entender tu postura de protección:

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

- **Protegido**: Se aplica una política. ARP (o ARP/AI según la versión de ONTAP) 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 habilitada una política de detección primaria, está "en riesgo" incluso si tiene habilitadas una política de instantáneas y de respaldo.
- **En progreso**: Se está aplicando una política pero aún no está completa.
- **Error**: Se aplica una política pero no funciona.

Estado de detección:

+ Ransomware Resilience proporciona información sobre el alcance de las políticas de detección de ransomware que has configurado en tus cargas de trabajo. Revisa el alcance de la detección con los siguientes campos.

- **Estado de detección de cifrado**
- **Estado de detección de comportamiento sospechoso de usuario**
- **Bloquea extensiones de archivo sospechosas**

Snapshot, replicación y backup policies: Esta columna muestra el producto o servicio que está gestionando la política. Si no hay política, el campo muestra N/A.

Importancia

Ransomware Resilience asigna una importancia o prioridad a cada carga de trabajo durante el descubrimiento basándose en un análisis de cada carga de trabajo. La importancia de la carga de trabajo está determinada por las siguientes frecuencias de instantáneas:

- **Crítico**: Se toma más de una copia de instantánea por hora (programa de protección altamente agresivo)
- **Importante**: Las copias instantáneas se crean con una frecuencia menor a cada hora, pero mayor a la de cada día.
- **Estándar**: Se toman copias instantáneas más de una vez al día

Exposición de privacidad: selecciona esta opción para "escanea información de identificación personal con NetApp Data Classification".

Destino de replicación: si has configurado la replicación de instantáneas, se muestran los nombres de las máquinas virtuales de almacenamiento y sistemas de destino. Si no hay replicación, este campo muestra "N/A".

Destino de la copia de seguridad: si has configurado una estrategia de protección contra ransomware con copias de seguridad, el nombre del sistema de destino de la copia de seguridad aparece aquí.

Próximos pasos

- "Proteja las cargas de trabajo con estrategias de protección contra ransomware"
- "Gestiona grupos de protección"
- "Escanear en busca de datos de identificación personal"

Proteja las cargas de trabajo con las estrategias de protección NetApp Ransomware Resilience

Las estrategias de protección contra el ransomware son una característica clave de NetApp Ransomware Resilience: apoyan la detección, protección y replicación. Las estrategias de protección son una pieza esencial de tu postura de ciberseguridad.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Comprender las estrategias de protección contra ransomware

Las estrategias de protección contra ransomware abarcan *detección*, *protección* y *replicación*.

- **Políticas de detección** identifican amenazas de ransomware
- **Las políticas de protección** incluyen políticas de instantáneas y de copia de seguridad. Se requieren políticas de detección y captura de instantáneas en una estrategia de protección. Las políticas de respaldo son opcionales.

  Si utiliza otros productos de NetApp para proteger su carga de trabajo, Ransomware Resilience los detecta y ofrece la opción de:

  - utilizar una política de detección de ransomware y continuar utilizando las políticas de instantáneas y copias de seguridad creadas por otras herramientas de NetApp , o
  - Utilice Ransomware Resilience para gestionar la detección, las instantáneas y las copias de seguridad.
- **Las políticas de replicación** le permiten replicar instantáneas de Ransomware Resilience a un sitio secundario. Los programas de replicación se pueden configurar con frecuencias horarias, diarias, semanales o mensuales.

  Actualmente, solo puedes replicar instantáneas en el almacenamiento ONTAP local.

Si estás configurando estrategias de protección para Amazon FSxN para ONTAP y Azure NetApp Files, consulta "las limitaciones de cada servicio".

Para mejorar la gestión y la protección de tu parque de datos, puedes crear "cargas de trabajo de grupo" para proteger colectivamente los volúmenes bajo una misma estrategia.

Políticas de protección con otros servicios administrados por NetApp

Además de Ransomware Resilience, puedes usar NetApp Backup and Recovery para gestionar la protección de archivos compartidos y archivos compartidos de VM.

La información de protección de los servicios de Backup & Recovery aparece en Ransomware Resilience. Puedes añadir políticas de detección a estos servicios con Ransomware Resilience. Añadir una política de protección con Ransomware Resilience reemplaza las políticas de protección existentes.

Ransomware Resilience también descubre políticas de protección de SnapCenter para VMware para almacenes de datos de VM y SnapCenter para Oracle. No puedes usar estos servicios para restaurar con Ransomware Resilience.

Si una política de detección de ransomware está siendo administrada por Autonomous Ransomware Protection (ARP o ARP/AI, según la versión de ONTAP) y FPolicy en ONTAP, esas cargas de trabajo están protegidas y continuarán siendo administradas por ARP y FPolicy.

Los destinos de backup no están disponibles para cargas de trabajo en Amazon FSx for NetApp ONTAP o Azure NetApp Files. Realiza operaciones de backup usando el servicio de backup de FSx for ONTAP. Configuras las políticas de backup para cargas de trabajo en FSx for ONTAP en AWS, no en Ransomware Resilience. Las políticas de backup aparecen en Ransomware Resilience y permanecen sin cambios desde AWS.

Políticas de protección para cargas de trabajo no protegidas por aplicaciones de NetApp

Si tu carga de trabajo no está gestionada por Backup and Recovery o Ransomware Resilience, es posible que tenga instantáneas tomadas como parte de ONTAP u otros productos. Si la protección de ONTAP FPolicy está implementada, puedes cambiar la protección de FPolicy usando ONTAP.

Políticas de detección predefinidas

Puede elegir una de las siguientes políticas predefinidas de resiliencia ante ransomware, que están alineadas con la importancia de la carga de trabajo.

La política **Extensión de usuario de cifrado** es la única política predefinida que admite la detección de comportamiento sospechoso de usuarios.

+ La **política de replicación crítica** es la única política predefinida que admite la replicación de instantáneas en ONTAP.

Nivel de política	Snapshot	Frecuencia	Retención (días)	Número de copias de instantáneas	Número máximo de copias de instantáneas
Política de carga de trabajo crítica	Cada cuarto de hora	Cada 15 minutos	3	288	309
	Diario	Cada 1 día	14	14	309
	Semanalmente	Cada 1 semana	35	5	309
	Mensual	Cada 30 días	60	2	309
Política de carga de trabajo importante	Cada cuarto de hora	Cada 30 minutos	3	144	165
	Diario	Cada 1 día	14	14	165
	Semanalmente	Cada 1 semana	35	5	165
	Mensual	Cada 30 días	60	2	165
Política de carga de trabajo estándar	Cada cuarto de hora	Cada 30 min	3	72	93
	Diario	Cada 1 día	14	14	93
	Semanalmente	Cada 1 semana	35	5	93
	Mensual	Cada 30 días	60	2	93
Extensión de usuario de cifrado	Cada cuarto de hora	Cada 30 min	3	72	93
	Diario	Cada 1 día	14	14	93
	Semanalmente	Cada 1 semana	35	5	93
	Mensual	Cada 30 días	60	2	93

Nivel de política	Snapshot	Frecuencia	Retención (días)	Número de copias de instantáneas	Número máximo de copias de instantáneas
Política de replicación crítica	Cada cuarto de hora	Cada 15 minutos	3	288	309
	Diario	Cada 1 día	14	14	309
	Semanalmente	Cada 1 semana	35	5	309
	Mensual	Cada 30 días	60	2	309

Agregar una estrategia de protección contra ransomware

Hay tres enfoques para agregar una estrategia de protección contra ransomware:

- **Cree una estrategia de protección contra ransomware si no tiene políticas de instantáneas o copias de seguridad.**

  La estrategia de protección contra ransomware incluye:

  - Política de instantáneas
  - Política de detección de ransomware
  - Política de respaldo

- **Sustituye las políticas de instantáneas o copias de seguridad existentes de Backup and Recovery protection por estrategias de protección gestionadas por Ransomware Resilience.**

  La estrategia de protección contra ransomware incluye:

  - Política de instantáneas
  - Política de detección de ransomware
  - Política de respaldo

- **Cree una política de detección para cargas de trabajo con políticas de backup e instantáneas existentes administradas en otros productos o servicios de NetApp .**

  La política de detección no cambia las políticas administradas en otros productos.

  La política de detección habilita la protección autónoma contra ransomware y la protección FPolicy si ya están activadas en otros servicios. Obtenga más información sobre"Protección autónoma contra ransomware" ,"Copia de seguridad y recuperación" , y"Política de ONTAP" .

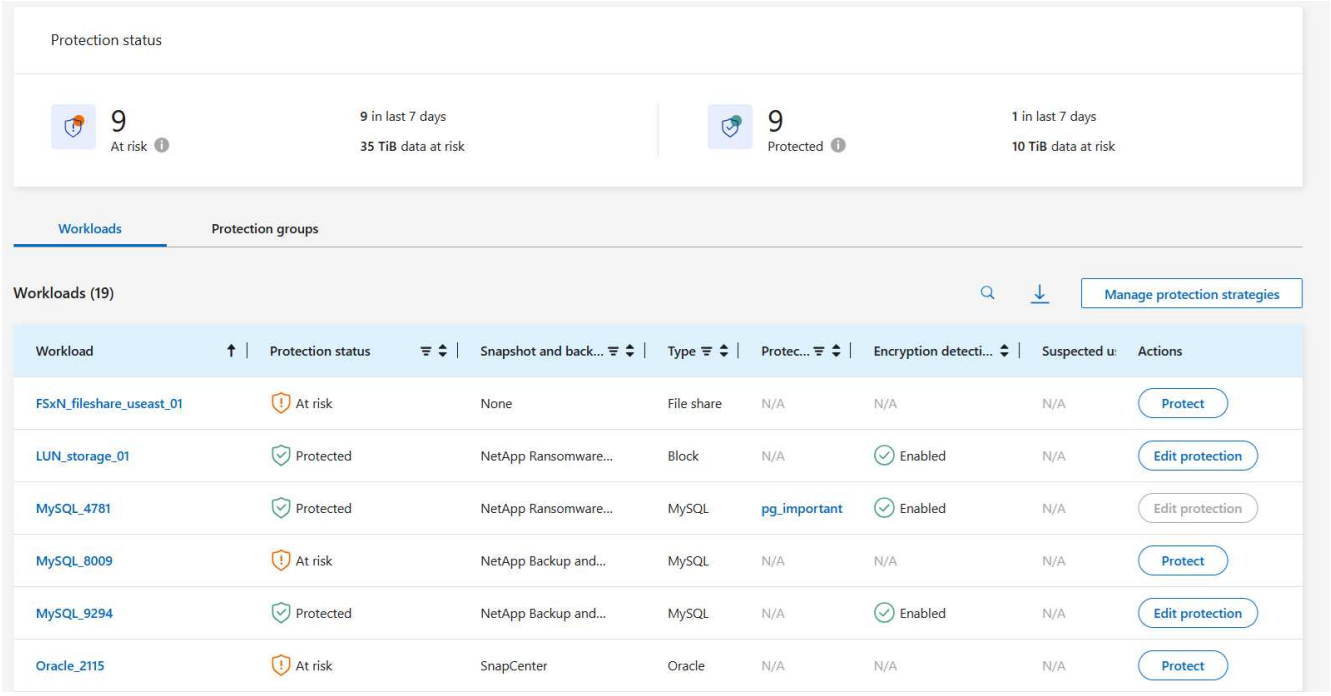
Cree una estrategia de protección contra ransomware (si no tiene políticas de instantáneas o copias de seguridad)

Si no existen políticas de instantáneas o de respaldo en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que cree en Ransomware Resilience:

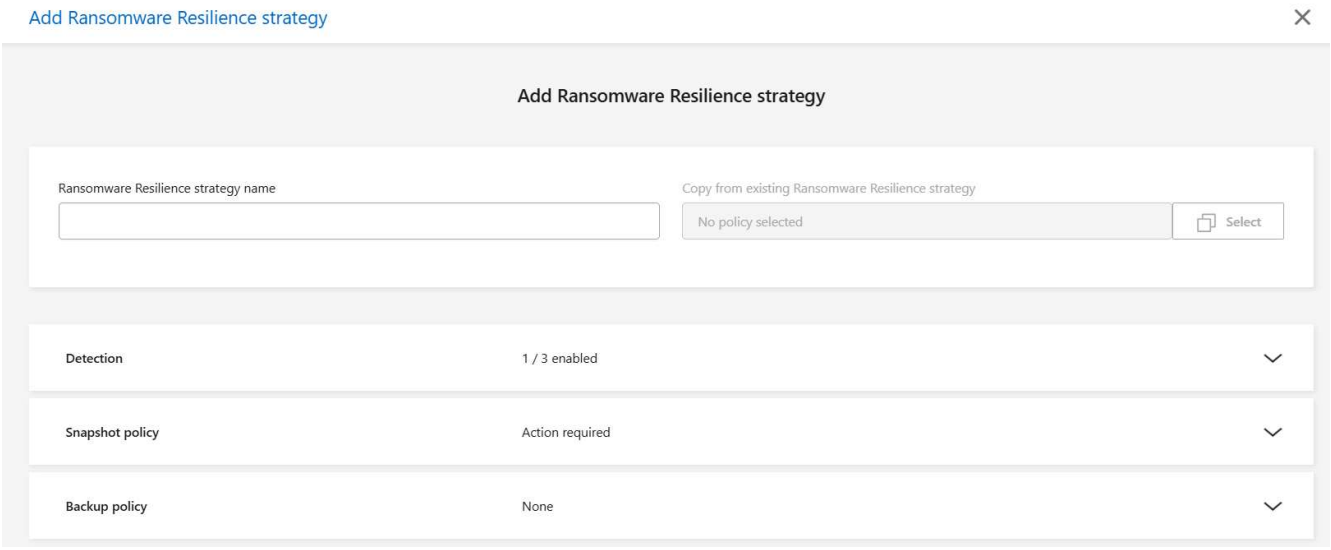
- Política de instantáneas
- Política de respaldo
- Política de detección de ransomware
- Replicación secundaria a ONTAP

Pasos para crear una estrategia de protección contra ransomware

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego **Proteger**.
3. Desde la página de estrategias de protección contra ransomware, seleccione **Agregar**.



4. Ingrese un nuevo nombre de estrategia o ingrese un nombre existente para copiarlo. Si ingresa un nombre existente, elija cuál desea copiar y seleccione **Copiar**.

Si elige copiar y modificar una estrategia existente, Ransomware Resilience agrega "_copy" al nombre original. Debes cambiar el nombre y al menos una configuración para que sea único.

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

   - **Política de detección**:
     - **Política**: Elija una de las políticas de detección prediseñadas.
     - **Detección primaria**: habilite Ransomware Resilience para detectar posibles ataques de ransomware.
     - **Detección de comportamiento sospechoso del usuario**: habilite la detección del comportamiento del usuario para transmitir eventos de actividad del usuario a Ransomware Resilience y detectar eventos sospechosos, como violaciones de datos.
     - **Bloquear extensiones de archivos**: habilite Ransomware Resilience para bloquear extensiones de archivos sospechosas conocidas. Ransomware Resilience toma copias instantáneas automáticas cuando la detección primaria está habilitada.

       Si desea cambiar las extensiones de archivos bloqueadas, edítelas en el Administrador del sistema.
   - **Política de instantáneas**:
     - **Nombre base de la política de instantánea**: seleccione una política o seleccione **Crear** e ingrese un nombre para la política de instantánea.
     - **Bloqueo de instantáneas**: habilite esta opción para bloquear las copias de instantáneas en el almacenamiento principal de modo que no se puedan modificar ni eliminar durante un período de tiempo determinado, incluso si un ataque de ransomware logra llegar al destino de almacenamiento de respaldo. Esto también se llama *almacenamiento inmutable*. Esto permite un tiempo de restauración más rápido.

       Cuando se bloquea una instantánea, el tiempo de expiración del volumen se establece en el tiempo de expiración de la copia de la instantánea.

   El bloqueo de copias instantáneas está disponible con ONTAP 9.12.1 y versiones posteriores. Para obtener más información sobre SnapLock, consulte "SnapLock en ONTAP" .

   - **Programaciones de instantáneas**: elija las opciones de programación, la cantidad de copias de instantáneas que desea conservar y seleccione para habilitar la programación.
     - **Política de replicación**:
   - **Nombre base de la política de replicación**: ingrese un nombre nuevo o elija uno existente. El nombre base es el prefijo que se añade a todas las instantáneas.
   - **Programaciones de replicación**: alterne las frecuencias que desea habilitar (por hora, por día, por semana o por mes) y configure el valor de retención (la cantidad de instantáneas replicadas que se conservarán) para cada programación que habilite.
     - **Política de respaldo**:
   - **Nombre base de la política de respaldo**: ingrese un nombre nuevo o elija uno existente.
   - **Programaciones de respaldo**: elija las opciones de programación para el almacenamiento secundario y habilite la programación.

Para habilitar el bloqueo de copias de seguridad en el almacenamiento secundario, configure los destinos de copia de seguridad utilizando la opción **Configuración**. Para obtener más información, consulte "Configurar ajustes" .

6. Seleccione **Agregar**.

Agrega una política de detección a las cargas de trabajo que ya tienen políticas de snapshot y backup gestionadas por Backup and Recovery

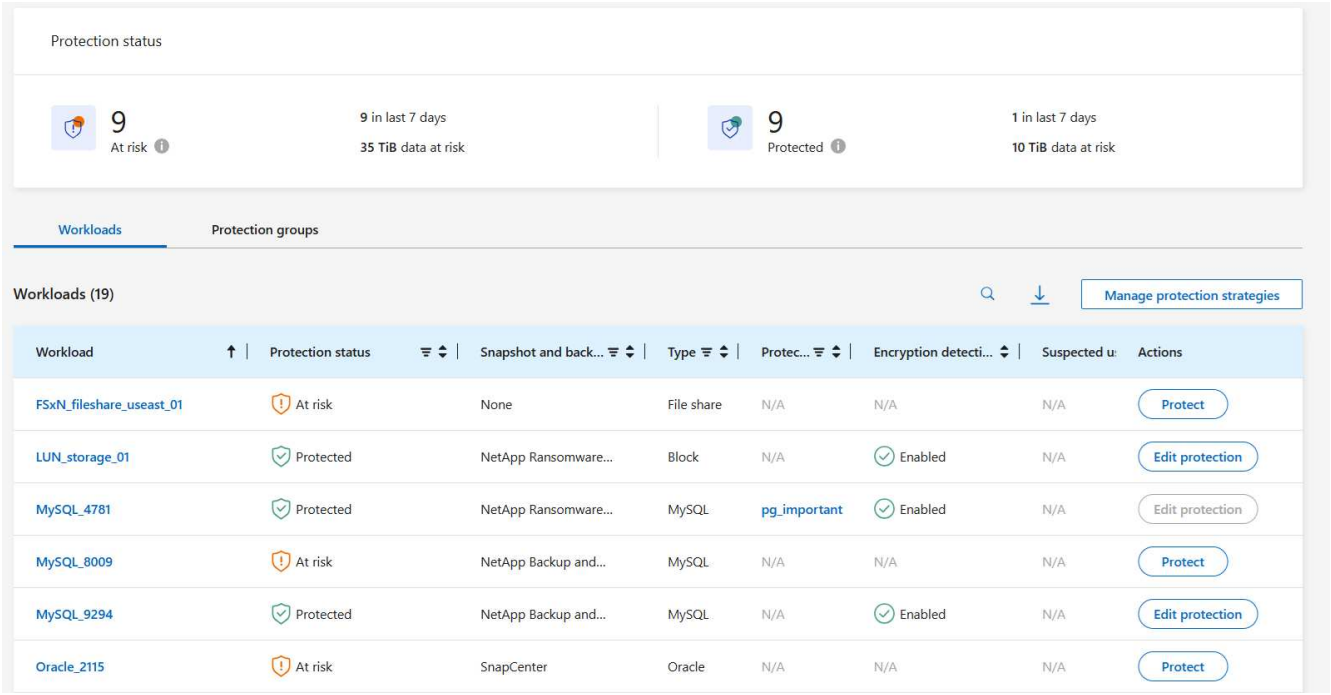
Ransomware Resilience te permite asignar una política de detección o una política de protección a cargas de trabajo con protección de instantáneas y copias de seguridad existente gestionada en otros productos o servicios de NetApp. Backup and Recovery usa políticas que rigen las instantáneas, la replicación a almacenamiento secundario o las copias de seguridad a almacenamiento de objetos.

Agregue una política de detección a las cargas de trabajo con políticas de copia de seguridad o instantáneas existentes

Si ya tienes políticas de instantáneas o copias de seguridad con Backup and Recovery, puedes añadir una política para detectar ataques de ransomware. Para gestionar la protección y la detección con Ransomware Resilience, consulta Protéjase con resiliencia contra ransomware.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego seleccione **Proteger**.
3. Ransomware Resilience detecta si hay políticas activas de Backup and Recovery.
4. Para dejar tu Backup and Recovery existente en su lugar y solo aplicar una política de *detección*, deja la casilla **Replace existing policies** sin marcar.
5. Selecciona la configuración de detección que quieras:
   - **Detección de cifrado**
   - **Detección de comportamiento sospechoso de usuario**

- **Bloquea extensiones de archivo sospechosas**

6. Seleccione **Siguiente**.
7. Si seleccionaste **Detección de comportamiento sospechoso del usuario** como configuración de detección, selecciona el User activity agent o "o crea uno".

   El agente de actividad del usuario aloja los nuevos recopiladores de datos. Ransomware Resilience crea automáticamente el recopilador de datos para transmitir eventos de actividad del usuario a Ransomware Resilience para detectar un comportamiento anómalo del usuario.

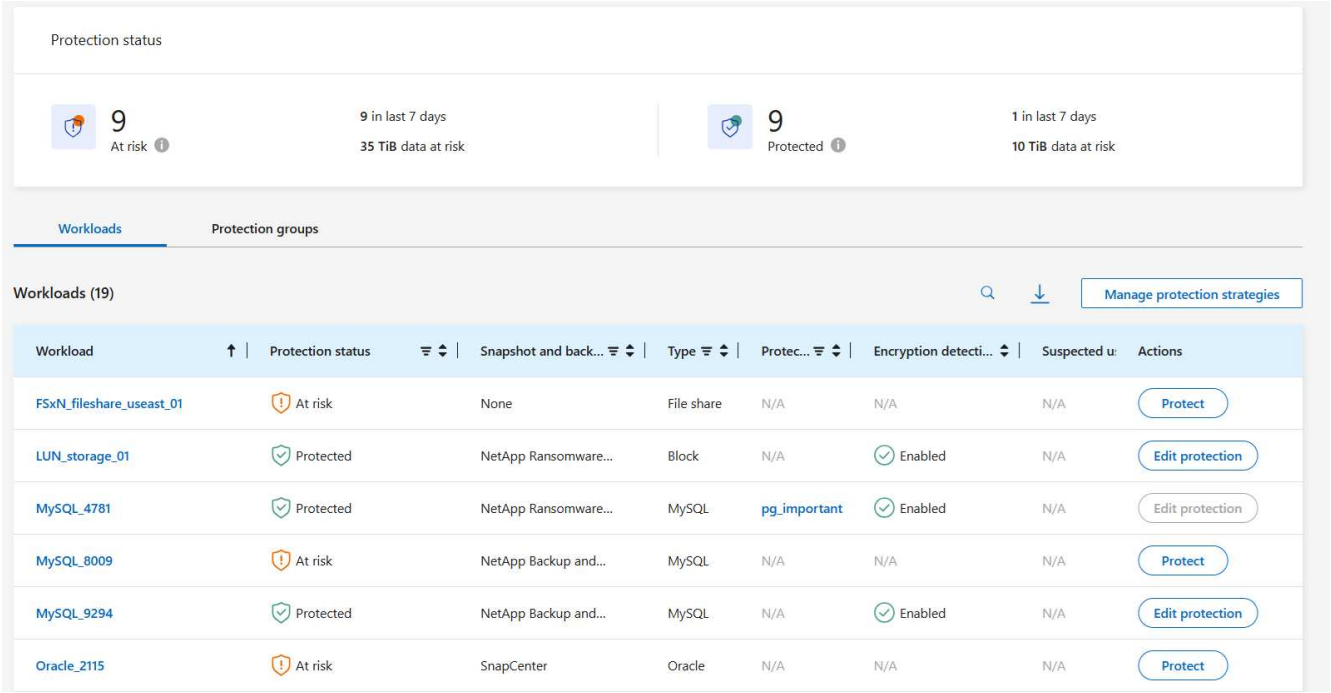
8. Seleccione **Siguiente**.
9. Revise sus opciones Seleccione **Crear** para activar la detección.
10. En la página Protección, revise el **Estado de detección** para confirmar que la detección esté Activa.

Reemplace las políticas de copia de seguridad o instantáneas existentes con una estrategia de protección contra ransomware

Puede reemplazar sus políticas de copia de seguridad o instantáneas existentes con una estrategia de protección contra ransomware. Este enfoque elimina la protección administrada externamente y configura la detección y protección en Ransomware Resilience.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde la página Protección, seleccione una carga de trabajo y luego seleccione **Proteger**.
3. Ransomware Resilience detecta si existen políticas activas de Backup and Recovery. Para reemplazar las políticas existentes, selecciona la casilla **Replace existing policies**. Cuando seleccionas la casilla, Ransomware Resilience reemplaza la lista de políticas de detección por políticas de detección.
4. Elija una política de protección. Si no existe ninguna política de protección, seleccione **Agregar** para crear una nueva política. Para obtener información sobre cómo crear una política, consulteCrear una política de protección . Seleccione **Siguiente**.

5. Si su estrategia incluye replicación, seleccione el **Sistema de destino** y la **VM de almacenamiento de destino**. Seleccione **Siguiente**.
6. Seleccione un destino de copia de seguridad o cree uno nuevo. Seleccione **Siguiente**.
    a. Si su estrategia de protección incluye la detección del comportamiento del usuario, seleccione un agente de actividad del usuario en su entorno para alojar los nuevos recopiladores de datos. Ransomware Resilience crea automáticamente el recopilador de datos para transmitir eventos de actividad del usuario a Ransomware Resilience para detectar un comportamiento anómalo del usuario.
7. Revise la nueva estrategia de protección y luego seleccione **Proteger** para aplicarla.
8. En la página Protección, revise el **Estado de detección** para confirmar que la detección esté Activa.

Asignar una política diferente

Puede reemplazar la política existente por una diferente.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, en la fila de carga de trabajo, seleccione **Editar protección**.
3. Si la carga de trabajo tiene una política de Backup and Recovery existente que quieres mantener, desmarca **Replace existing policies**. Para reemplazar las políticas existentes, marca **Replace existing policies**.
4. En la página Políticas, seleccione la flecha hacia abajo de la política que desea asignar para revisar los detalles.
5. Seleccione la política que desea asignar.
6. Seleccione **Proteger** para completar el cambio.

Gestionar estrategias de protección contra ransomware

Puedes eliminar una estrategia de ransomware.

Ver cargas de trabajo protegidas por una estrategia de protección contra ransomware

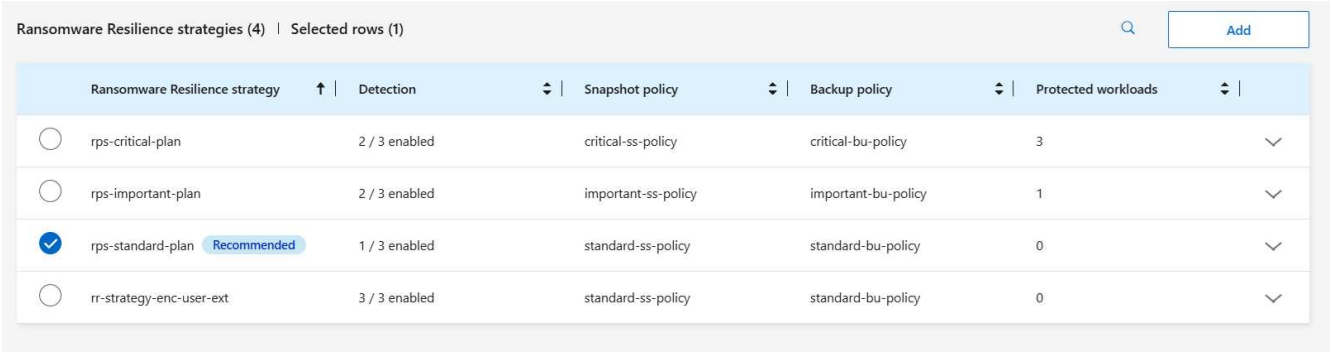
Antes de eliminar una estrategia de protección contra ransomware, es posible que desee ver qué cargas de trabajo están protegidas por esa estrategia.

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

Pasos para visualizar estrategias

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione **Administrar estrategias de protección**.

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



3. En la página Estrategias de protección contra ransomware, en la columna Cargas de trabajo protegidas, seleccione la flecha hacia abajo al final de la fila.

Eliminar una estrategia de protección contra ransomware

Puede eliminar una estrategia de protección que actualmente no esté asociada con ninguna carga de trabajo.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione **Administrar estrategias de protección**.
3. En la página Administrar estrategias, seleccione *Acciones* Opción para la estrategia que desea eliminar.
4. En el menú Acciones, seleccione **Eliminar política**.

Administra los grupos de protección en NetApp Ransomware Resilience

NetApp Ransomware Resilience ofrece grupos de protección para facilitar la gestión de tu patrimonio de datos. Los grupos de protección son agrupaciones lógicas de cargas de trabajo. Ransomware Resilience puede proteger todos los volúmenes de un grupo de protección al mismo tiempo con una sola estrategia de protección, así no tienes que aplicar una estrategia a cada carga de trabajo.

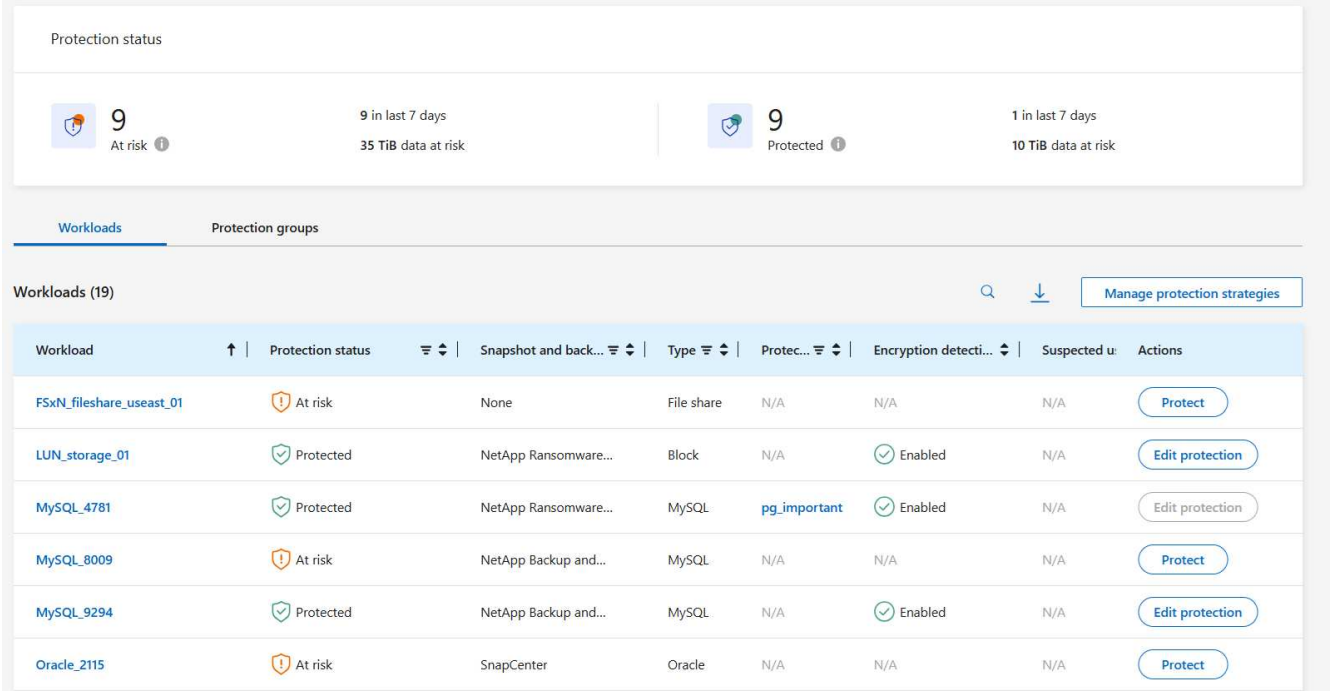
Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Crear un grupo de protección

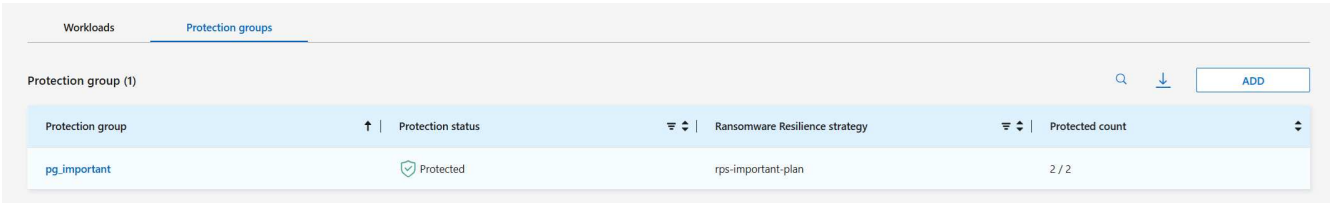
Puedes crear grupos independientemente de su estado de protección (es decir, grupos no protegidos y grupos protegidos). Cuando añades una política de protección a un grupo de protección, la nueva política de protección reemplaza cualquier política existente, incluidas las políticas gestionadas por NetApp Backup and Recovery.

Pasos

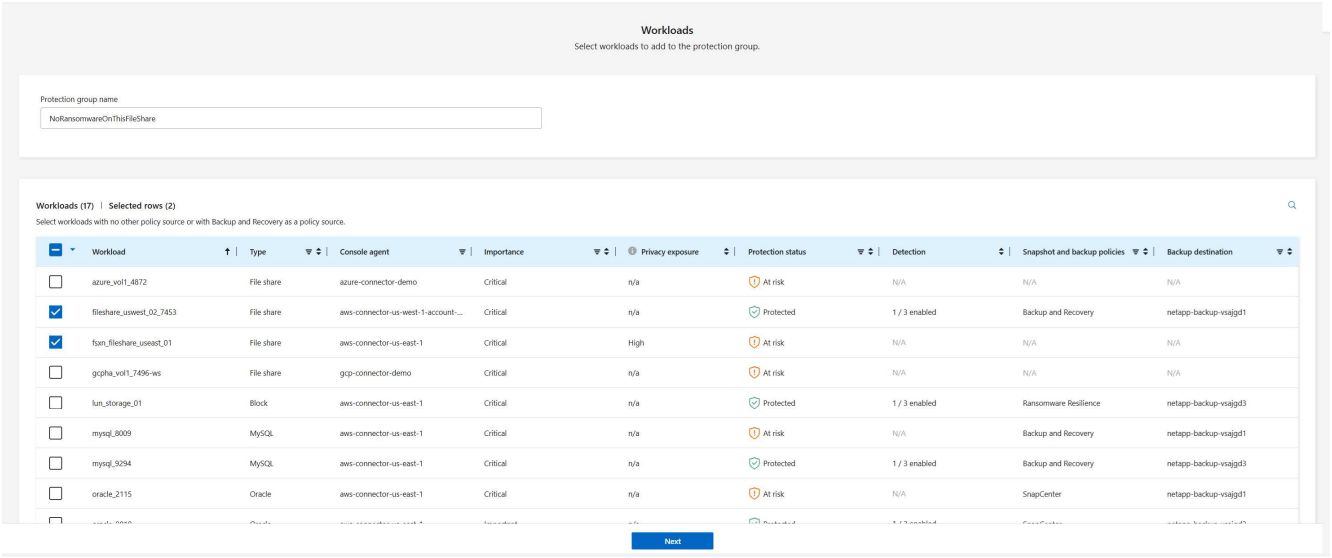
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.



2. Desde el panel Protección, selecciona la pestaña **Protection groups**.



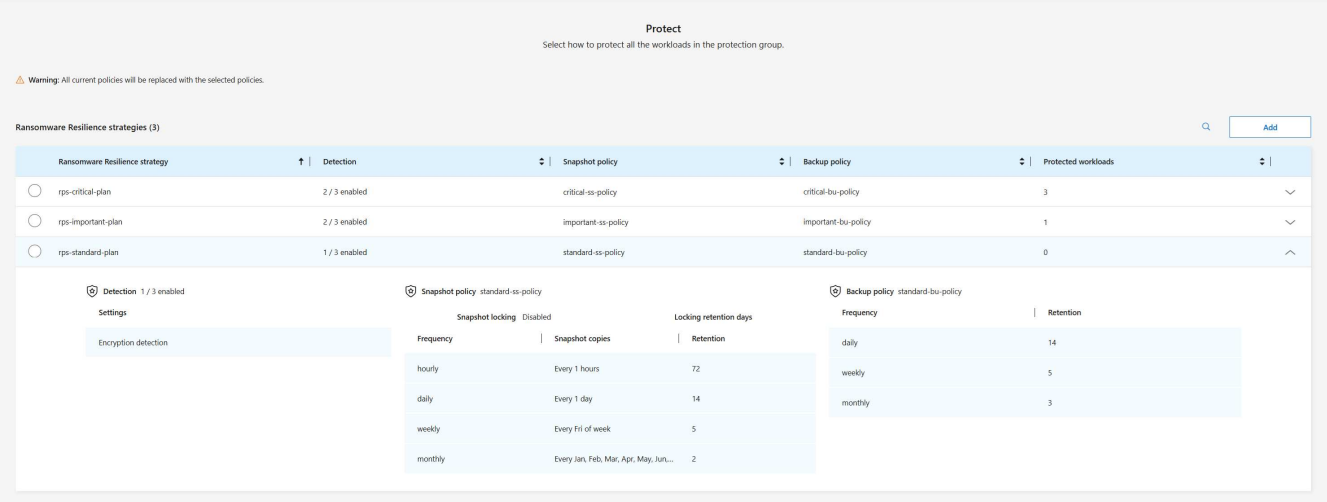
3. Seleccione **Agregar**.



4. Introduzca un nombre para el grupo de protección.
5. Seleccione las cargas de trabajo que desea agregar al grupo.

Para ver más detalles sobre las cargas de trabajo, desplácese hacia la derecha.

6. Seleccione **Siguiente**.



7. Selecciona una estrategia de protección para el grupo.
8. Si la estrategia de protección incluye replicación, revise la configuración de replicación.
    a. Para replicar todas las instantáneas en el mismo destino, marque **Usar el mismo destino para cada carga de trabajo**. Seleccione un **Sistema de destino** y una **VM de almacenamiento de destino** para las cargas de trabajo en la sección Agente de consola. + Para utilizar destinos diferentes, desmarque esa casilla. Revise cada carga de trabajo bajo cada agente de consola y asigne un **Sistema de destino** y una **VM de almacenamiento de destino** para cada carga de trabajo. Seleccione **Siguiente**.
9. Para configurar una política de respaldo, elija una y luego seleccione **Siguiente**.
10. Si su política de detección incluye la detección del comportamiento del usuario, seleccione el recopilador de datos que desea utilizar y luego **Siguiente**.
11. Revise las selecciones para el grupo de protección.
12. Para finalizar el grupo de protección, selecciona **Add**.

Al revisar el panel de protección en Ransomware Resilience, puedes ordenar las cargas de trabajo por grupo de protección.

Editar la protección del grupo

Puede cambiar la política de detección en un grupo existente.

Pasos

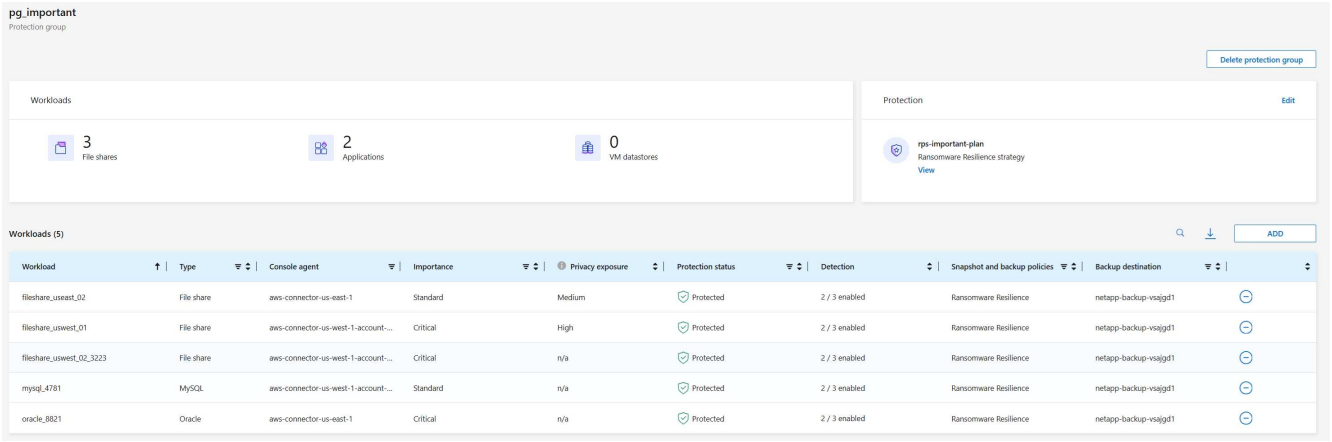
1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección** y luego seleccione el grupo cuya política desea modificar.
3. Desde la página de descripción general del grupo de protección, seleccione **Editar protección**.
4. Selecciona una política de protección existente para aplicarla o selecciona **Add** para crear una nueva política de protección. Para más información sobre cómo añadir una política de protección, consulta "Crear una política de protección". Luego selecciona **Save**.
5. En la descripción general del destino de copia de seguridad, seleccione un destino de copia de seguridad existente o **Agregar un nuevo destino de copia de seguridad**.
6. Seleccione **Siguiente** para revisar sus cambios.

Eliminar cargas de trabajo de un grupo de protección

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

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del cual desea eliminar una o más cargas de trabajo.



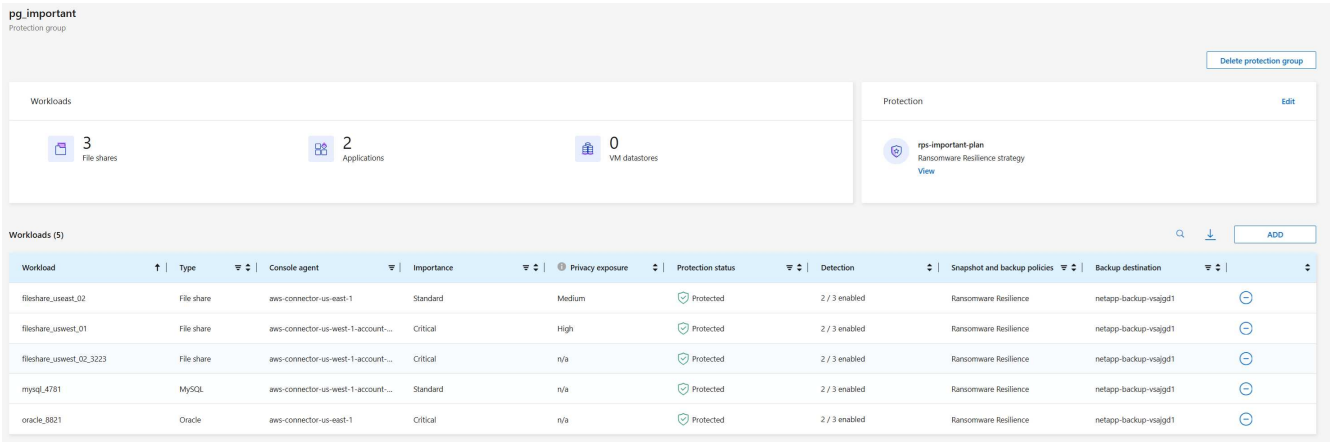
4. En la página del grupo de protección, selecciona la carga de trabajo que quieres quitar del grupo y selecciona la opción **Actions** ⋯.
5. En el menú Acciones, seleccione **Eliminar carga de trabajo**.
6. Confirme que desea eliminar la carga de trabajo y seleccione **Eliminar**.

Eliminar un grupo de protección

Cuando eliminas un grupo de protección, Ransomware Resilience elimina el grupo y la estrategia de protección de las cargas de trabajo. No elimina las cargas de trabajo individuales.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. Desde la página Protección, seleccione la pestaña **Grupos de protección**.
3. Seleccione el grupo del cual desea eliminar una o más cargas de trabajo.



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

Busque información de identificación personal con la NetApp Data Classification en Ransomware Resilience

Dentro de NetApp Ransomware Resilience, puede utilizar NetApp Data Classification para escanear y clasificar los datos en una carga de trabajo de uso compartido de archivos. La clasificación de datos le ayuda a determinar si el conjunto de datos incluye información de identificación personal (PII), lo que puede aumentar los riesgos de seguridad. La clasificación de datos es un componente central de la NetApp Console y está disponible sin costo adicional.

"Clasificación de datos"Utiliza el procesamiento del lenguaje natural impulsado por IA para el análisis y la categorización de datos contextuales, proporcionando información útil sobre sus datos para abordar los requisitos de cumplimiento, detectar vulnerabilidades de seguridad, optimizar costos y acelerar la migración.

Este proceso puede afectar la importancia de la carga de trabajo para ayudar a garantizar que tenga la protección adecuada.

Rol de consola requerido Para realizar esta tarea, necesita el rol de administrador de organización, administrador de carpeta o proyecto, o administrador de resiliencia ante ransomware. "Obtenga información sobre las funciones de resiliencia ante ransomware para la NetApp Console" .

Identificar la exposición a la privacidad con la clasificación de datos

Antes de utilizar la clasificación de datos dentro de Ransomware Resilience, necesita"para permitir que la clasificación de datos escanee sus datos" .

Puede implementar la clasificación de datos dentro de la página de Protección de Resiliencia contra ransomware. Siga el procedimiento para identificar la exposición a la privacidad. Cuando selecciona **Identificar exposición**, si aún no ha implementado la Clasificación de datos, un cuadro de diálogo le permitirá habilitarla.

Para obtener más información sobre la clasificación de datos, consulte:

- "Aprenda sobre la clasificación de datos"
- "Categorías de datos privados"
- "Investigue los datos almacenados en su organización"

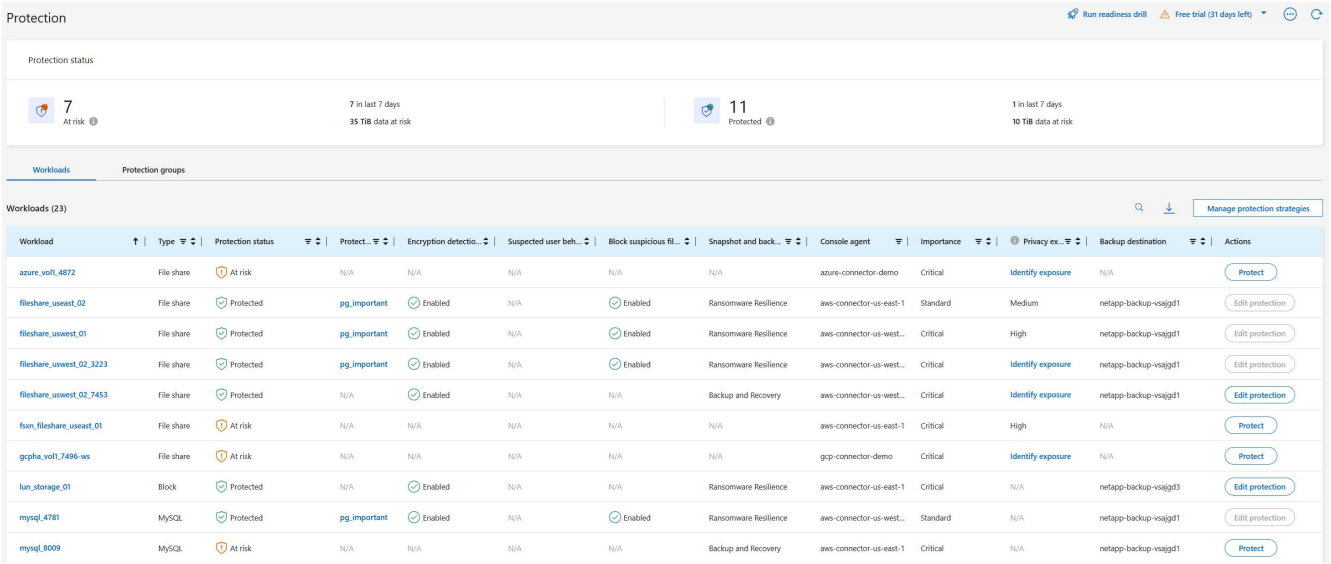
Antes de empezar

El escaneo de datos PII en Ransomware Resilience está disponible si tiene"Clasificación de datos implementada" . La clasificación de datos está disponible como parte de la consola sin costo adicional y se puede implementar en las instalaciones o en la nube del cliente.

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. En la página Protección, busque una carga de trabajo de uso compartido de archivos en la columna Carga

de trabajo.



3. Para habilitar la Clasificación de datos para escanear sus datos en busca de información personal identificable, en la columna **Exposición de privacidad**, seleccione **Identificar exposición**.

> Si no ha implementado la Clasificación de datos, al seleccionar **Identificar exposición** se abre un cuadro de diálogo para implementar la Clasificación de datos. Seleccione **Implementar**. Después de haber implementado la Clasificación de datos, puede regresar a la página Protección y luego seleccionar **Identificar exposición**.

Resultado

El escaneo puede tardar varios minutos dependiendo del tamaño y la cantidad de archivos. Durante el escaneo, la página de Protección indica que está identificando archivos y proporciona un recuento de archivos. Una vez finalizado el escaneo, la columna Exposición a la privacidad clasifica el nivel de exposición como Bajo, Medio o Alto.

Revisar la exposición a la privacidad

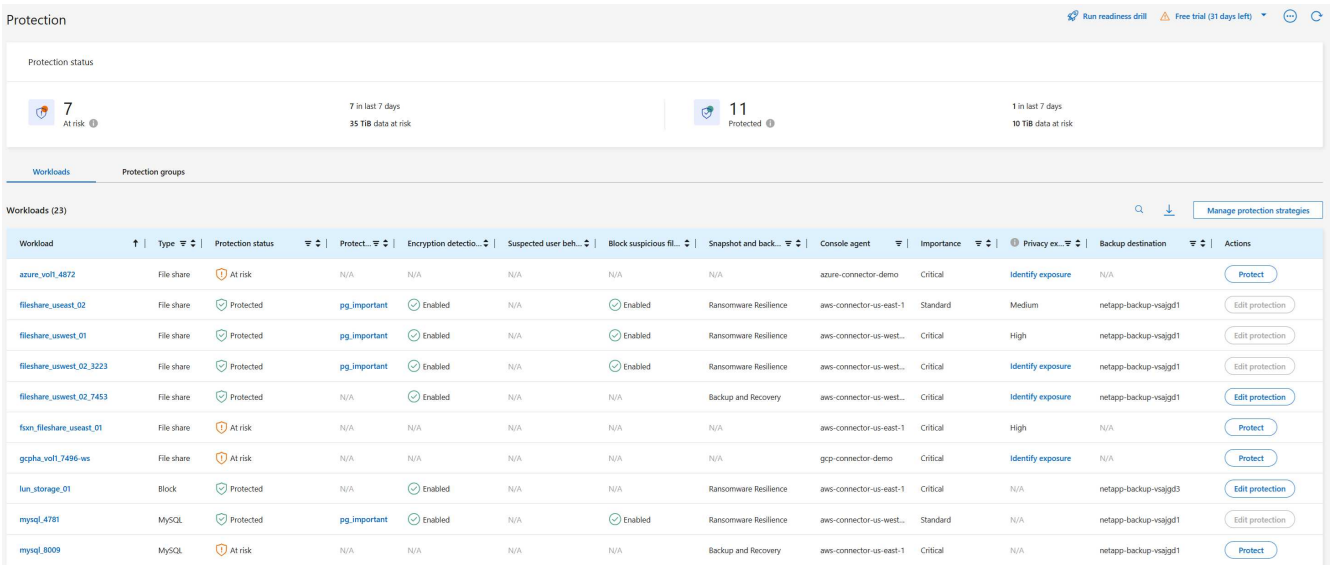
Después de los análisis de clasificación de datos en busca de información personal identificable, evalúe el riesgo.

Los datos PII se clasifican en una de tres designaciones:

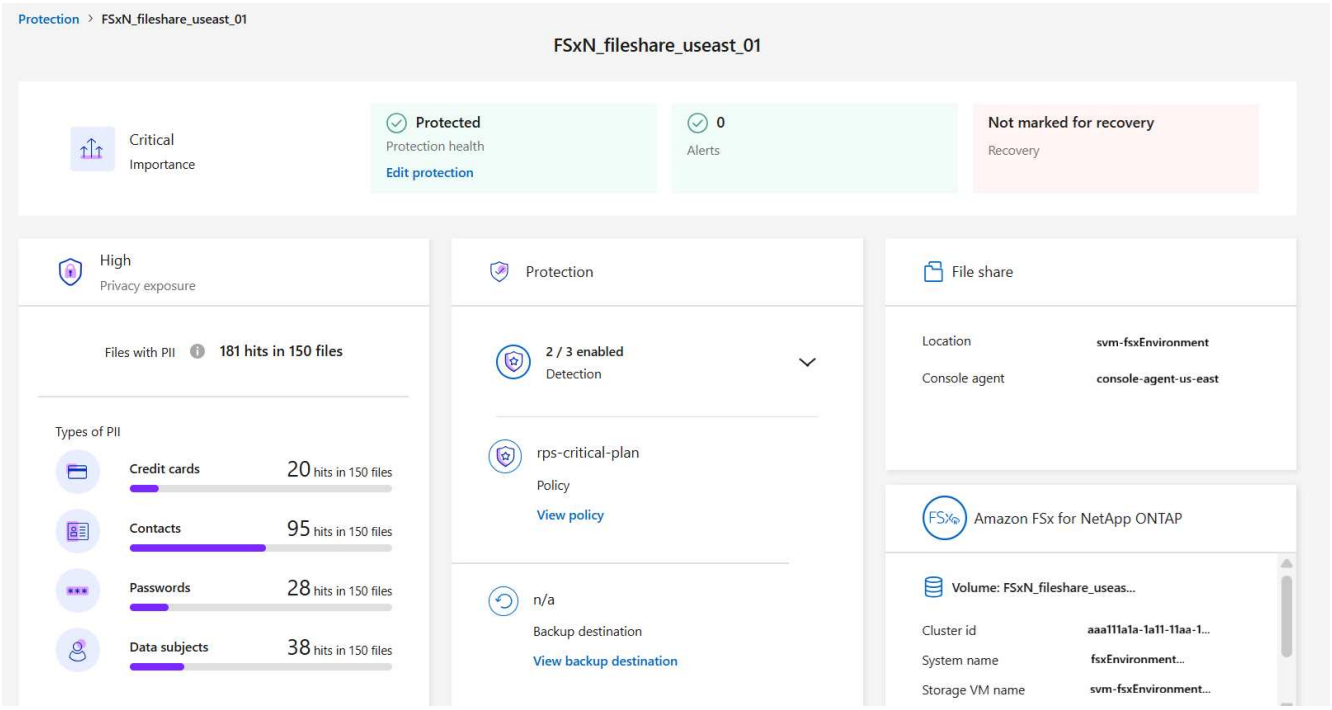
- **Alto**: Más del 70% de los archivos contienen información personal identificable
- **Medio**: Más del 30% y menos del 70% de los archivos contienen información de identificación personal (PII)
- **Bajo**: Más del 0% y menos del 30% de los archivos contienen información personal identificable

Pasos

1. En el menú Resiliencia ante ransomware, seleccione **Protección**.
2. En la página Protección, ubique la carga de trabajo del recurso compartido de archivos en la columna Carga de trabajo que muestra un estado en la columna Exposición de privacidad.



3. Seleccione el enlace de carga de trabajo en la columna Carga de trabajo para ver los detalles de la carga de trabajo.



4. En la página de detalles de la carga de trabajo, observe los detalles en el mosaico de exposición de privacidad.

El impacto de la exposición a la privacidad en la importancia de la carga de trabajo

Los cambios en la exposición a la privacidad pueden afectar la importancia de la carga de trabajo.

Cuando se expone la privacidad:	De esta exposición de privacidad:	A esta exposición de privacidad:	Entonces, la importancia de la carga de trabajo hace esto: .
Disminuye	Alto, Medio o Bajo	Medio, bajo o ninguno	Sigue igual
Aumenta	Ninguno	Bajo	Permanece en Standard
	Bajo	Medio	Cambios de Estándar a Importante
	Bajo o medio	Alto	Cambios de Estándar o Importante a Crítico

Para más información

Para obtener detalles sobre la clasificación de datos, consulte la documentación de clasificación de datos:

- "Aprenda sobre la clasificación de datos"
- "Categorías de datos privados"
- "Investigue los datos almacenados en su organización"