Empezar

NetApp Ransomware Resilience

NetApp
March 12, 2026

Tabla de contenidos

Empezar

Obtenga más información sobre la NetApp Ransomware Resilience

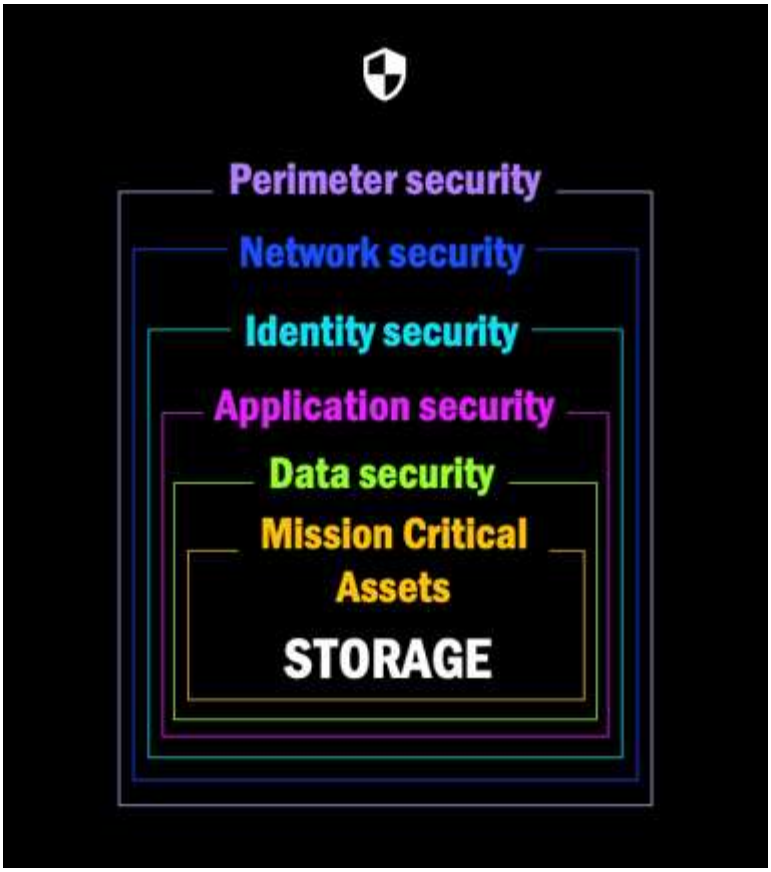
Los ataques de ransomware pueden bloquear el acceso a sus datos y los atacantes pueden pedir un rescate a cambio de la liberación de datos o el descifrado. Según IDC, no es raro que las víctimas de ransomware experimenten múltiples ataques de ransomware. El ataque puede interrumpir el acceso a sus datos durante un período que puede durar desde un día hasta varias semanas.

NetApp Ransomware Resilience protege tus datos de los ataques de ransomware. En Ransomware Resilience, la protección está disponible para cargas de trabajo basadas en aplicaciones de Oracle, almacenes de datos de VM y archivos compartidos para almacenamiento NAS (protocolos NFS y CIFS) y almacenamiento SAN (protocolos FC, iSCSI y NVMe). Ransomware Resilience es compatible con el almacenamiento local, así como con Cloud Volumes ONTAP para Amazon Web Services, Cloud Volumes ONTAP para Google Cloud, Cloud Volumes ONTAP para Microsoft Azure, Azure NetApp Files y Amazon FSx for NetApp ONTAP a través de la NetApp Console. Puedes hacer backup de datos en Amazon Web Services, Google Cloud, Microsoft Azure y NetApp StorageGRID.

Resiliencia frente al ransomware en la capa de datos

Su postura de seguridad generalmente abarca múltiples capas de defensa para protegerse contra una variedad de amenazas cibernéticas.

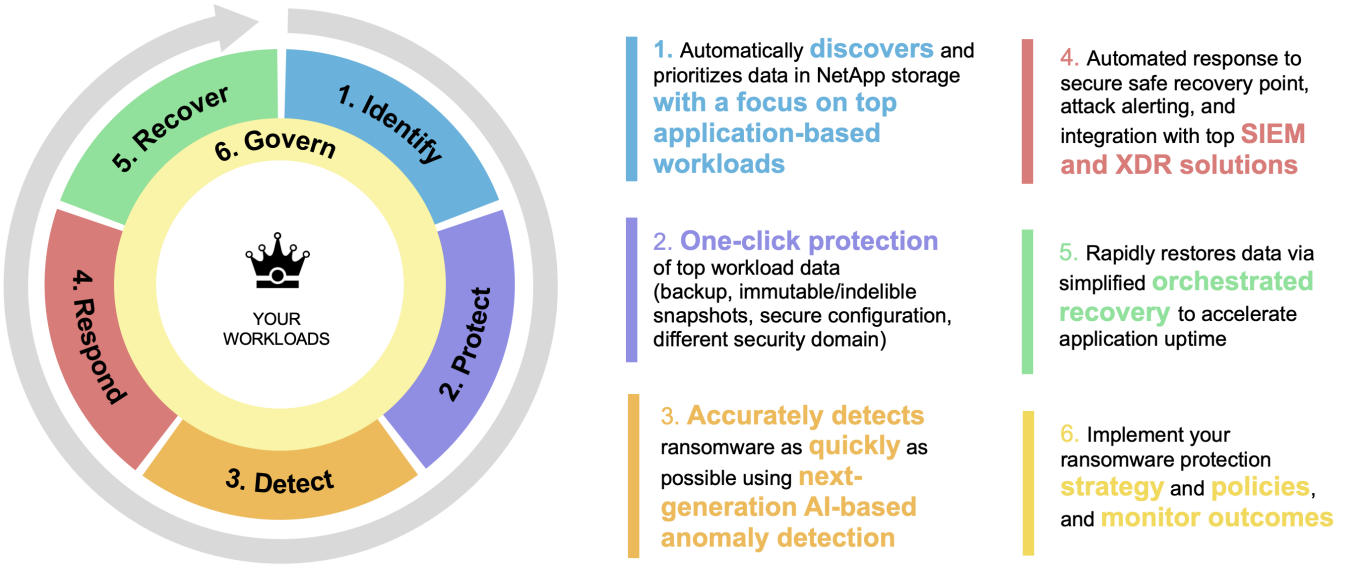
- **Capa más externa**: esta es su primera línea de defensa, que utiliza firewalls, sistemas de detección de intrusiones y redes privadas virtuales para proteger los límites de la red.
- **Seguridad de la red**: esta capa se basa en la base con segmentación de red, monitoreo de tráfico y cifrado.
- **Seguridad de identidad**: utiliza métodos de autenticación, controles de acceso y gestión de identidad para garantizar que solo los usuarios autorizados puedan acceder a recursos confidenciales.
- **Seguridad de la aplicación**: protege las aplicaciones de software mediante prácticas de codificación segura, pruebas de seguridad y autoprotección de aplicaciones en tiempo de ejecución.
- **Seguridad de datos**: protege tus datos con protección de datos, copias de seguridad y estrategias de recuperación. La resiliencia frente al ransomware opera en esta capa.



Qué puedes hacer con Ransomware Resilience

Ransomware Resilience proporciona el uso completo de varias tecnologías de NetApp para que su administrador de almacenamiento, administrador de seguridad de datos o ingeniero de operaciones de seguridad puedan lograr los siguientes objetivos:

- **Identifica** cargas de trabajo basadas en aplicaciones, archivos compartidos o gestionadas por VMware en sistemas NAS y SAN locales de NetApp a través de la NetApp Console, proyectos y agentes de Console. Después de descubrir las cargas de trabajo, Ransomware Resilience identifica oportunidades para mejorar la resiliencia frente al ransomware.
- **Proteja** sus cargas de trabajo habilitando copias de seguridad, copias instantáneas y estrategias de protección contra ransomware en sus datos.
- **Detectar** anomalías que podrían ser ataques de ransomware. Nota al pie: [Si bien es posible que un ataque pase desapercibido, nuestra investigación indica que la tecnología de NetApp ha dado como resultado un alto grado de detección para ciertos ataques de ransomware basados en cifrado de archivos].
- **Responder** a posibles ataques de ransomware iniciando automáticamente una instantánea de un punto en el tiempo que se bloquea para que la copia no pueda eliminarse de manera accidental o maliciosa. Sus datos de respaldo permanecerán inmutables y protegidos de extremo a extremo contra ataques de ransomware en el origen y en el destino.
- **Recupere** sus cargas de trabajo que ayudan a acelerar el tiempo de actividad de la carga de trabajo mediante la orquestación de varias tecnologías de NetApp . Puede elegir recuperar volúmenes específicos. Ransomware Resilience ofrece recomendaciones sobre las mejores opciones.
- **Gobernar**: Implemente su estrategia de protección contra ransomware y monitoree los resultados.



Beneficios de utilizar Ransomware Resilience

La resiliencia frente al ransomware ofrece los siguientes beneficios:

- Descubre cargas de trabajo y sus programaciones de instantáneas y copias de seguridad existentes, y clasifica su importancia relativa.
- Evalúa tu postura de protección frente al ransomware y la muestra en un panel de control fácil de entender mientras te da recomendaciones para mejorar la protección.
- Aplica recomendaciones de protección de datos impulsadas por IA/ML con acceso con un solo clic.
- Protege datos en cargas de trabajo basadas en aplicaciones, como Oracle, almacenes de datos de VMware y recursos compartidos de archivos.
- Detecta ataques de ransomware a datos en tiempo real en el almacenamiento primario utilizando tecnología de IA.
- Inicia acciones automatizadas en respuesta a posibles ataques detectados creando copias instantáneas e iniciando alertas sobre actividad anormal.
- Aplica la recuperación curada para cumplir las políticas de RPO. Ransomware Resilience orquesta la recuperación de incidentes de ransomware por NetApp Backup and Recovery.
- Utiliza el control de acceso basado en roles (RBAC) para gobernar el acceso a funciones y operaciones.

Costo

Puedes probar Ransomware Resilience con una prueba gratuita de 30 días. NetApp no le cobra por utilizar la versión de prueba de Ransomware Resilience.

Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos productos se factura únicamente por Ransomware Resilience.

Cuando una carga de trabajo se clasifica como protegida, cuenta contra la capacidad adquirida o la suscripción PAYGO. Ransomware Resilience clasifica una carga de trabajo como protegida cuando se habilita una política de detección con al menos una política de instantáneas o de backup. Las cargas de trabajo descubiertas con una política de detección pero *sin* políticas de backup o instantáneas se clasifican como en riesgo. Las cargas de trabajo en riesgo no cuentan contra la capacidad adquirida.

Las cargas de trabajo protegidas cuentan contra la capacidad adquirida o la suscripción después de que termine el periodo de prueba gratuito. Ransomware Resilience se cobra por GB para los datos asociados con las cargas de trabajo protegidas (según lo reporta ONTAP) antes de las eficiencias.

Licencias

Con Ransomware Resilience, puede utilizar diferentes planes de licencia, incluida una prueba gratuita, una suscripción de pago por uso o traer su propia licencia.

La resiliencia contra ransomware requiere una licencia de NetApp ONTAP One.

La licencia Ransomware Resilience no incluye productos NetApp adicionales. Ransomware Resilience puede utilizar Backup and Recovery incluso si no tiene una licencia para ello.

Para detectar un comportamiento anómalo del usuario, Ransomware Resilience utiliza NetApp Autonomous Ransomware Protection, un modelo de aprendizaje automático (ML) dentro de ONTAP que detecta la actividad de archivos maliciosos. Este modelo está incluido en la licencia Ransomware Resilience.

Para obtener más información, consulte "Configurar licencias" .

NetApp Console

Se puede acceder a Ransomware Resilience a través de la NetApp Console.

La NetApp Console proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp . Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

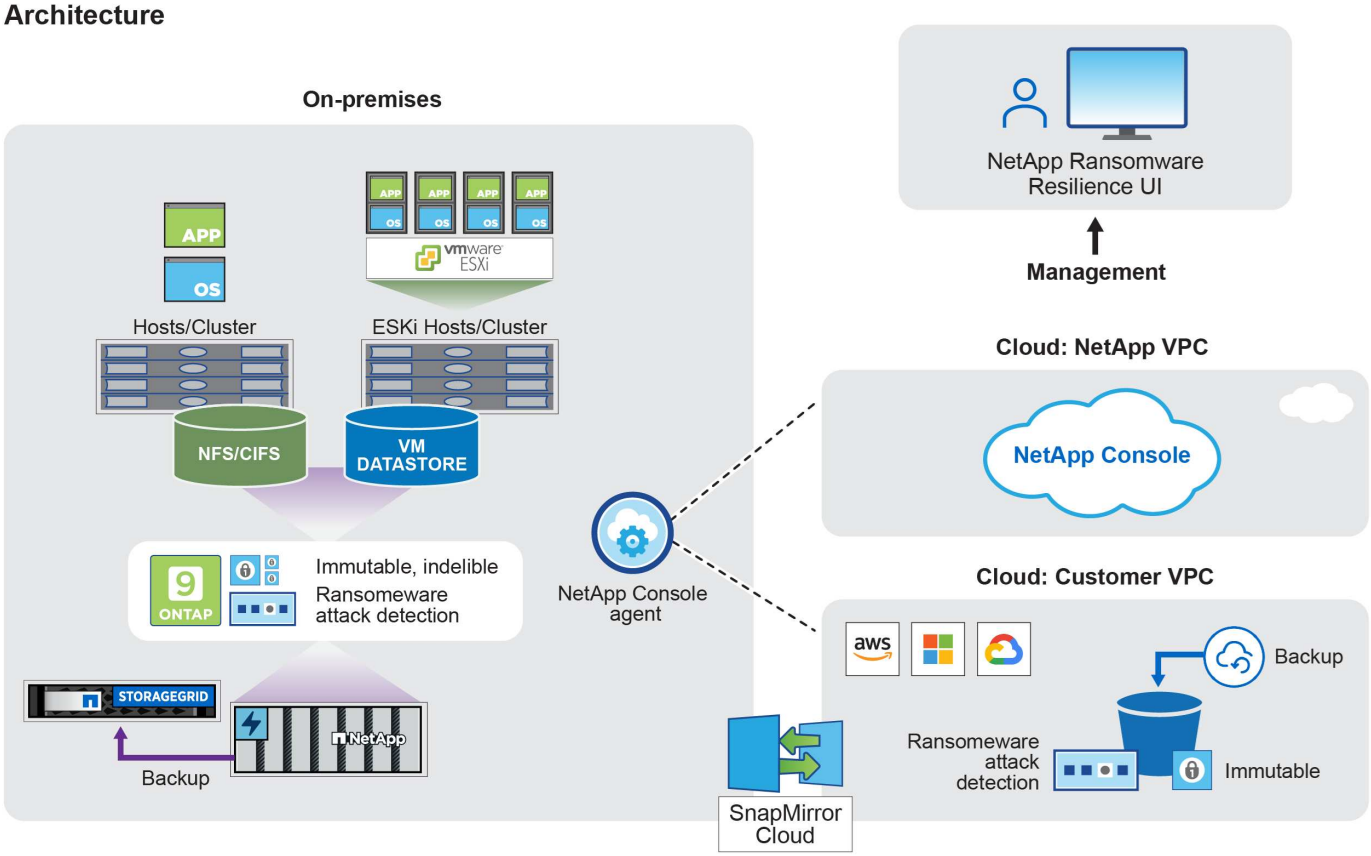
No necesitas una licencia ni suscripción para empezar a usar NetApp Console y solo incurres en cargos cuando despliegas agentes de Console en tu nube para asegurar la conectividad con tus sistemas de almacenamiento o servicios de datos de NetApp. Sin embargo, algunos servicios de datos de NetApp accesibles desde Console tienen licencia o requieren suscripción.

Obtenga más información sobre el"NetApp Console" .

Cómo funciona la resiliencia frente al ransomware

Ransomware Resilience utiliza NetApp Backup and Recovery para descubrir y establecer políticas de instantáneas y copias de seguridad para cargas de trabajo de archivos compartidos.

Architecture



Característica	Descripción
IDENTIFICAR	• Encuentra todos los datos NAS (NFS y CIFS) y SAN (FC, iSCSI y NVMe) locales y en la nube del cliente en sistemas conectados a la Console. • Identifica los datos del cliente de las API de ONTAP y NetApp Backup and Recovery y los asocia con las cargas de trabajo. Más información sobre "ONTAP". • Descubre el nivel de protección actual de cada volumen de las copias de instantáneas de NetApp y las políticas de respaldo, así como también cualquier capacidad de detección integrada. Luego, Ransomware Resilience asocia esta postura de protección con las cargas de trabajo mediante el uso de Backup and Recovery, servicios ONTAP y tecnologías de NetApp como Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP), FPolicy, políticas de backup y políticas de snapshots. Obtenga más información sobre "Protección autónoma contra ransomware" , "NetApp Backup and Recovery" , y "Política de ONTAP" . • Asigna una prioridad comercial a cada carga de trabajo en función de los niveles de protección descubiertos automáticamente y recomienda políticas de protección para las cargas de trabajo en función de su prioridad comercial. La prioridad de la carga de trabajo se basa en las frecuencias de instantáneas ya aplicadas a cada volumen asociado con la carga de trabajo.
PROTEGER	• Supervisa activamente las cargas de trabajo y orquesta el uso de las API de Backup and Recovery y ONTAP aplicando políticas a cada una de las cargas de trabajo identificadas.

Característica	Descripción
DETECTAR	• Detecta ataques potenciales con un modelo de aprendizaje automático (ML) integrado que detecta actividad y cifrado potencialmente anómalos. • Proporciona detección de doble capa que comienza con la detección de posibles ataques de ransomware en el almacenamiento principal y responde a actividades anormales tomando copias instantáneas automatizadas adicionales para crear los puntos de restauración de datos más cercanos. Ransomware Resilience proporciona la capacidad de profundizar para identificar ataques potenciales con mayor precisión sin afectar el rendimiento de las cargas de trabajo principales. • Determina los archivos sospechosos específicos y los asigna a las cargas de trabajo asociadas, utilizando ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y tecnologías FPolicy.
RESPONDER	• Muestra datos relevantes, como la actividad del archivo, la actividad del usuario y la entropía, para ayudarlo a completar revisiones forenses sobre el ataque. • Inicia copias instantáneas rápidas mediante el uso de tecnologías y productos de NetApp , como ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y FPolicy.
RECUPERAR	• Determina la mejor instantánea o copia de seguridad y recomienda el mejor punto de recuperación real (RPA) mediante el uso de Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI según su versión de ONTAP) y tecnologías y servicios de FPolicy. • Orquesta la recuperación de cargas de trabajo, incluidas máquinas virtuales, recursos compartidos de archivos, almacenamiento en bloque y bases de datos con consistencia de aplicaciones.
GOBERNAR	• Asigna las estrategias de protección contra ransomware • Le ayuda a monitorear los resultados.

Destinos de copia de seguridad, sistemas y fuentes de datos de carga de trabajo compatibles

Ransomware Resilience admite los siguientes objetivos de respaldo, sistemas y fuentes de datos:

Destinos de copia de seguridad compatibles

- Servicios web de Amazon (AWS) S3
- Plataforma de Google Cloud
- Blob de Microsoft Azure
- StorageGRID en NetApp

Sistemas compatibles

Ambiente	Protocolo	Versiones compatibles
Amazon FSx for NetApp ONTAP*	CIFS, NFS y SAN	N/A

Ambiente	Protocolo	Versiones compatibles
Azure NetApp Files	CIFS y NFS	N/A
Cloud Volumes ONTAP para AWS	CIFS y NFS	9.11.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Google Cloud Platform	CIFS y NFS	9.11.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Microsoft Azure	CIFS y NFS	9.12.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
ONTAP (en las instalaciones)	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores

* Amazon FSx for NetApp ONTAP utiliza la Protección Autónoma contra el Ransomware (ARP) y no ARP/AI. Para obtener más información sobre la diferencia, consulte"ARP/IA" .

El uso de ARP/AI en ONTAP requiere ONTAP 9.16 o superior. + ONTAP no proporciona soporte de protección contra ransomware para FabricPool FlexCache, volúmenes FlexGroup , volúmenes de punto de montaje de grupos de consistencia, volúmenes de ruta de montaje, volúmenes sin conexión y volúmenes de protección de datos (DP). Asegúrese de revisar"Configuraciones admitidas y no admitidas en ONTAP" .

Fuentes de datos de carga de trabajo compatibles

Ransomware Resilience protege las siguientes cargas de trabajo basadas en aplicaciones en volúmenes de datos primarios:

- Almacenamiento en bloque
- Bases de datos:
  - Microsoft SQL Server
  - Oráculo
  - PostgreSQL
- Recursos compartidos de archivos de NetApp
- Almacenes de datos de VMware

Términos clave

Podría resultarle beneficioso comprender cierta terminología relacionada con la protección contra ransomware.

- **Protección**: La protección contra ransomware significa garantizar que se realicen instantáneas y copias de seguridad inmutables de forma regular en un dominio de seguridad diferente mediante políticas de protección.
- **Carga de trabajo**: una carga de trabajo en Ransomware Resilience puede incluir bases de datos de Oracle, almacenes de datos de VMware o recursos compartidos de archivos.

Requisitos previos de NetApp Ransomware Resilience

Para garantizar el éxito de la implantación de NetApp Ransomware Resilience, verifica que tu entorno operativo, el acceso a la red y el navegador web estén listos.

Revisa y asegúrate de cumplir con los siguientes requisitos.

Sistemas compatibles

Asegúrese de estar utilizando un sistema compatible:

Ambiente	Protocolo	Versiones compatibles
Amazon FSx for NetApp ONTAP*	CIFS, NFS y SAN	N/A
Azure NetApp Files	CIFS y NFS	N/A
Cloud Volumes ONTAP para AWS	CIFS y NFS	9.11.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Google Cloud Platform	CIFS y NFS	9.11.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
Cloud Volumes ONTAP para Microsoft Azure	CIFS y NFS	9.12.1 y posteriores
	SAN (iSCSI y NVMe)	9.17.1 y posteriores
ONTAP (en las instalaciones)	CIFS y NFS	9.11.1 y posteriores
	SAN (FC, iSCSI y NVMe)	9.17.1 y posteriores

* Amazon FSx for NetApp ONTAP utiliza la Protección Autónoma contra el Ransomware (ARP) y no ARP/AI. Para obtener más información sobre la diferencia, consulte"ARP/IA" .

Requisitos de la NetApp Console

La configuración de su NetApp Console requiere:

- Una cuenta de usuario de la NetApp Console con privilegios de administrador de la organización para descubrir recursos.
- Una organización y sistema de consola con al menos un agente de consola activo conectado a una"sistema compatible" .
  - Si tus clústeres ONTAP locales o sistemas Cloud Volumes ONTAP no están configurados en la NetApp Console, consulta "Aprenda a configurar un agente de consola" y "Requisitos estándar de la consola".

> Si tiene varios agentes de consola en una sola organización de consola, Ransomware Resilience escaneará los recursos de ONTAP en todos los agentes de consola más allá del que esté seleccionado actualmente en la interfaz de usuario de la consola.

- El agente de consola debe tener la `cloudmanager-ransomware-protection` contenedor en estado activo.
- Para clústeres ONTAP o Cloud Volumes ONTAP, Ransomware Resilience requiere que la versión de

ONTAP sea 9.11.1 o mayor.

> Para utilizar la resiliencia contra el ransomware en cargas de trabajo SAN, debe estar ejecutando ONTAP 9.17.1 o posterior.

Requisitos de ONTAP

- Debe estar ejecutando ONTAP 9.11.1 o posterior con una licencia ONTAP One habilitada en la instancia ONTAP local. Para obtener más información sobre la compatibilidad con ONTAP , consulte"Descripción general de la protección autónoma contra ransomware" .
- Para aplicar configuraciones de protección (como habilitar la protección autónoma contra ransomware), Ransomware Resilience necesita permisos de administrador en el clúster ONTAP . El clúster ONTAP debería haberse incorporado utilizando únicamente las credenciales de usuario administrador del clúster ONTAP .

> Si ha conectado un clúster ONTAP a la consola con credenciales que no son de administrador, [debe actualizar las credenciales en el clúster ONTAP](#update-non-admin-user-permissions-in-an-ontap-system).

Copias de seguridad de datos

- Una cuenta en NetApp StorageGRID, AWS S3, Azure Blob o Google Cloud Platform para destinos de copia de seguridad con los permisos de acceso adecuados configurados.

  Consulte la "Lista de permisos de AWS, Azure o S3" Para más detalles.

- No es necesario habilitar NetApp Backup and Recovery en el sistema.

  Ransomware Resilience te ayuda a configurar un destino de backup usando la opción de configuración. Mira "Agregar un destino de respaldo".

Requisitos de comportamiento sospechoso del usuario

Para que Ransomware Resilience te dé alertas sobre comportamientos sospechosos de usuarios, debes configurar un agente de actividad de usuario. Para instalar un agente de actividad de usuario, asegúrate de que tu sistema cumple "los requisitos".

Actualizar los permisos de usuarios no administradores en un sistema ONTAP

Si necesitas actualizar los permisos de usuarios que no son administradores para un sistema en particular, usa estos pasos.

1. Inicia sesión en la Console. En el dashboard, identifica el sistema que necesita que se actualicen sus permisos de usuario de ONTAP.
2. Selecciona el sistema para ver sus detalles.
3. Seleccione **Ver información adicional** para mostrar el nombre de usuario.
4. Inicie sesión en la CLI del clúster ONTAP como usuario administrador.
5. Muestra los roles existentes para ese usuario:

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

6. Cambiar el rol del usuario. Ingresar:

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

7. Vuelva a la NetApp Console para usar la función de resiliencia ante ransomware.

Inicio rápido para la NetApp Ransomware Resilience

Comprenda los pasos de alto nivel que debe seguir para configurar Ransomware Resilience y proteger sus cargas de trabajo.

Siga los enlaces en cada paso para obtener información detallada.

1 Revisar los prerrequisitos

Estas tareas requieren el rol de *Administrador de consola*.

- "Asegúrese de haber instalado un agente de consola"
- "Asegúrese de que su sistema cumpla con los requisitos"
- "Revise los roles de usuario de Ransomware Resilience y asigne permisos a los usuarios que acceden a Ransomware Resilience"
- "Configurar licencias"

2 Comience a utilizar Ransomware Resilience

Estas tareas requieren el rol de *administrador de resiliencia ante ransomware*.

- "Descubra cargas de trabajo en la consola"
- "Ver el estado de protección de la carga de trabajo en el Panel de control"
- "Opcionalmente, realice un simulacro de preparación para un ataque de ransomware."

3 Configurar la protección y detección en Ransomware Resilience

Estas tareas requieren el rol de *administrador de resiliencia ante ransomware*. Para configurar la actividad de comportamiento de usuario sospechoso se requiere el rol adicional *Administrador de comportamiento de usuario de Ransomware Resilience*.

- "Proteger las cargas de trabajo"
  - Opcionalmente,"Mejore la protección configurando la detección de actividad sospechosa del usuario"
- Opcionalmente, configure los destinos de respaldo:

    - "Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform o Microsoft Azure como destino de respaldo" .
    - "Configurar destinos de respaldo"
- "Responder a la detección de posibles ataques de ransomware"
- "Recuperarse de un ataque (después de que se neutralizan los incidentes)"

4 **¿Que sigue?**

Después de configurar la protección en Ransomware Resilience, esto es lo que puede hacer a continuación.

- "Habilitar la clasificación de datos para identificar riesgos de gobernanza y seguridad"
- "Enviar alertas a SIEM"
- "Descargue informes de alerta, protección, simulacro de preparación, recuperación o resumen"

Configurar NetApp Ransomware Resilience

Puede implementar NetApp Ransomware Resilience fácilmente. Antes de comenzar, revise"prerrequisitos" para garantizar que su entorno esté preparado.

Preparar el destino de la copia de seguridad

Prepare uno de los siguientes destinos de respaldo:

- StorageGRID en NetApp
- Servicios web de Amazon
- Plataforma de Google Cloud
- Microsoft Azure

Después de configurar las opciones en el propio destino de backup, luego lo vas a configurar como destino de backup en Ransomware Resilience. Para detalles sobre cómo configurar el destino de backup en Ransomware Resilience, consulta "Configurar destinos de respaldo".

Prepare StorageGRID para que se convierta en un destino de respaldo

Si desea utilizar StorageGRID como destino de su copia de seguridad, consulte "Documentación de StorageGRID" para obtener detalles sobre StorageGRID.

Prepare AWS para convertirse en un destino de respaldo

- Configurar una cuenta en AWS.
- Configurar "Permisos de AWS" en AWS.

Para obtener detalles sobre cómo administrar su almacenamiento de AWS en la consola, consulte "Administra tus buckets de Amazon S3" .

Prepare Azure para convertirse en un destino de respaldo

- Configurar una cuenta en Azure.

- Configurar "Permisos de Azure" en Azure.

Para obtener detalles sobre cómo administrar su almacenamiento de Azure en la consola, consulte "Administrar sus cuentas de almacenamiento de Azure" .

Configurar la NetApp Console

El siguiente paso es configurar la consola y la resiliencia contra ransomware.

Revisar "Requisitos de consola para el modo estándar" .

Crear un agente de consola

Comuníquese con su representante de ventas de NetApp para probar o utilizar este servicio. Luego, cuando utilice el agente de consola, incluirá las capacidades adecuadas para la resiliencia ante ransomware.

Para crear un agente de consola mediante Ransomware Resilience, comuníquese con el administrador de su organización de consola que tenga permisos para crear agentes de consola y consulte la documentación que describe "Cómo crear un agente de consola" .

> Si tiene varios agentes de consola, los datos del análisis de resiliencia contra ransomware se recopilan en todos los agentes de consola más allá del que se muestra actualmente en la consola. Este servicio descubre todos los proyectos y todos los agentes de consola asociados con esta organización.

Configurar licencias para NetApp Ransomware Resilience

NetApp Ransomware Resilience ofrece diferentes planes de licencia, lo que te permite suscribirte al servicio donde tenga sentido para tu organización.

Para configurar las licencias, necesitas el rol de administrador de organización, carpeta o proyecto. "Obtenga más información sobre los roles de acceso a la consola".

Tipos de licencia

La resiliencia ante el ransomware está disponible con los siguientes tipos de licencia:

- Prueba gratuita de 30 días
- Compre una suscripción de pago por uso (PAYGO) con Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace o Azure Marketplace
- Traiga su propia licencia (BYOL): un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en la consola.

Después de configurar su BYOL o comprar una suscripción PAYGO, podrá ver la licencia en la sección Licenses and subscriptions de la Consola.

Una vez finalizada la prueba gratuita o vencida la licencia o suscripción, aún puedes:

- Ver cargas de trabajo y el estado de las cargas de trabajo
- Eliminar recursos como políticas
- Ejecute todas las operaciones programadas creadas durante el período de prueba o bajo la licencia

Otras licencias

La licencia Ransomware Resilience no incluye productos NetApp adicionales. Sin embargo, Ransomware Resilience puede integrarse con NetApp Backup and Recovery, incluso si no tiene una licencia separada para Backup and Recovery.

Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos productos se facturará únicamente por Ransomware Resilience.

Costo

Si tiene Backup and Recovery y Ransomware Resilience, cualquier dato común protegido por ambos productos se factura únicamente por Ransomware Resilience.

Cuando una carga de trabajo se clasifica como protegida, cuenta contra la capacidad adquirida o la suscripción PAYGO. Ransomware Resilience clasifica una carga de trabajo como protegida cuando se habilita una política de detección con al menos una política de instantáneas o de backup. Las cargas de trabajo descubiertas con una política de detección pero *sin* políticas de backup o instantáneas se clasifican como en riesgo. Las cargas de trabajo en riesgo no cuentan contra la capacidad adquirida.

Las cargas de trabajo protegidas cuentan contra la capacidad adquirida o la suscripción después de que termine el periodo de prueba gratuito. Ransomware Resilience se cobra por GB para los datos asociados con las cargas de trabajo protegidas (según lo reporta ONTAP) antes de las eficiencias.

Supervisa el tamaño de los datos protegidos en el panel de protección de Ransomware Resilience. Para añadir capacidad, consulta "Actualizar una licencia".

Pruebe Ransomware Resilience con una prueba gratuita de 30 días

Puedes probar Ransomware Resilience con una prueba gratuita de 30 días. Debes ser administrador de la organización de la consola para comenzar la prueba gratuita.

Los límites de capacidad de almacenamiento no se aplican durante la prueba.

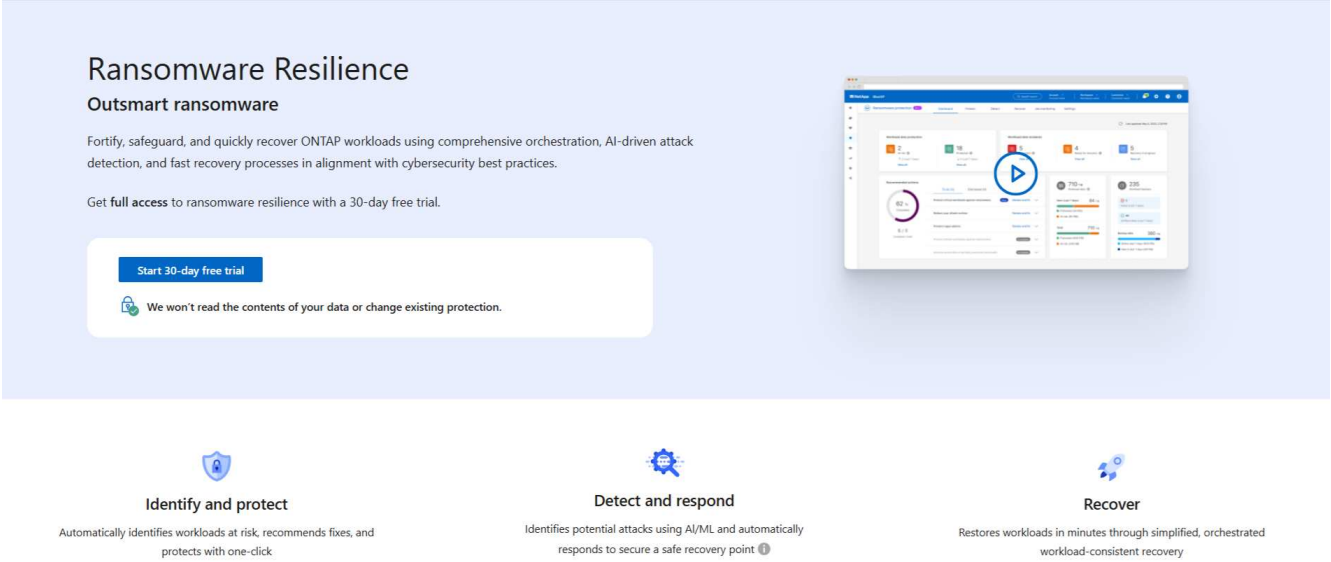
Puede obtener una licencia o suscribirse en cualquier momento y no se le cobrará hasta que finalice la prueba de 30 días. Para continuar después de la prueba de 30 días, deberá comprar una licencia BYOL o una suscripción PAYGO.

Durante la prueba, tendrás acceso a todas las funciones.

Pasos

1. Acceder a la "Consola" .
2. Inicie sesión en la consola.
3. Desde la NetApp Console, seleccione **Protección** > **Resiliencia contra ransomware**.

   Si es la primera vez que inicia sesión en este servicio, aparecerá la página de destino.



4. Si aún no ha agregado un agente de consola para otros servicios,"añadir uno" .
5. En la página de inicio de Resiliencia contra ransomware, seleccione **Comenzar por descubrir cargas de trabajo** para descubrir sus cargas de trabajo.

   Esta opción solo está disponible si ha instalado correctamente un agente de consola.

6. Para revisar la información de la prueba gratuita, seleccione la opción desplegable en la parte superior derecha.

Una vez finalizada la prueba, obtén una suscripción o licencia

Una vez finalizada la prueba gratuita, puedes suscribirte a través de uno de los Marketplaces o comprar una licencia de NetApp.

Si ya tiene una suscripción PAYGO, la licencia se cambia automáticamente a la suscripción una vez finalizada la prueba gratuita.

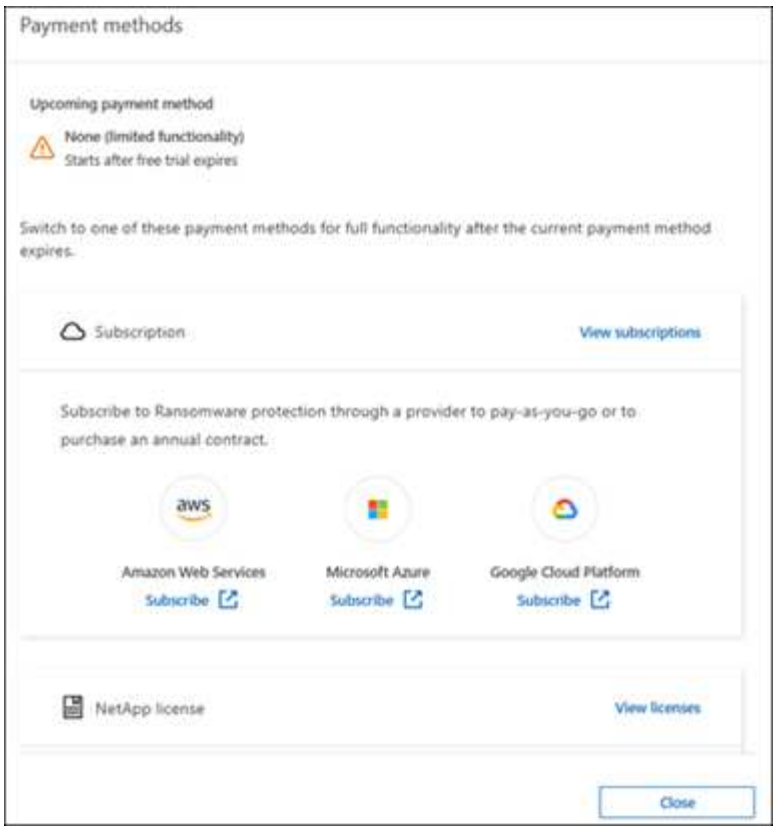
Suscríbete a través de AWS Marketplace Suscríbete a través de Microsoft Azure Marketplace Suscríbete a través de Google Cloud Platform Marketplace Traiga su propia licencia (BYOL)

Suscríbete a través de AWS Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en AWS Marketplace.

Pasos

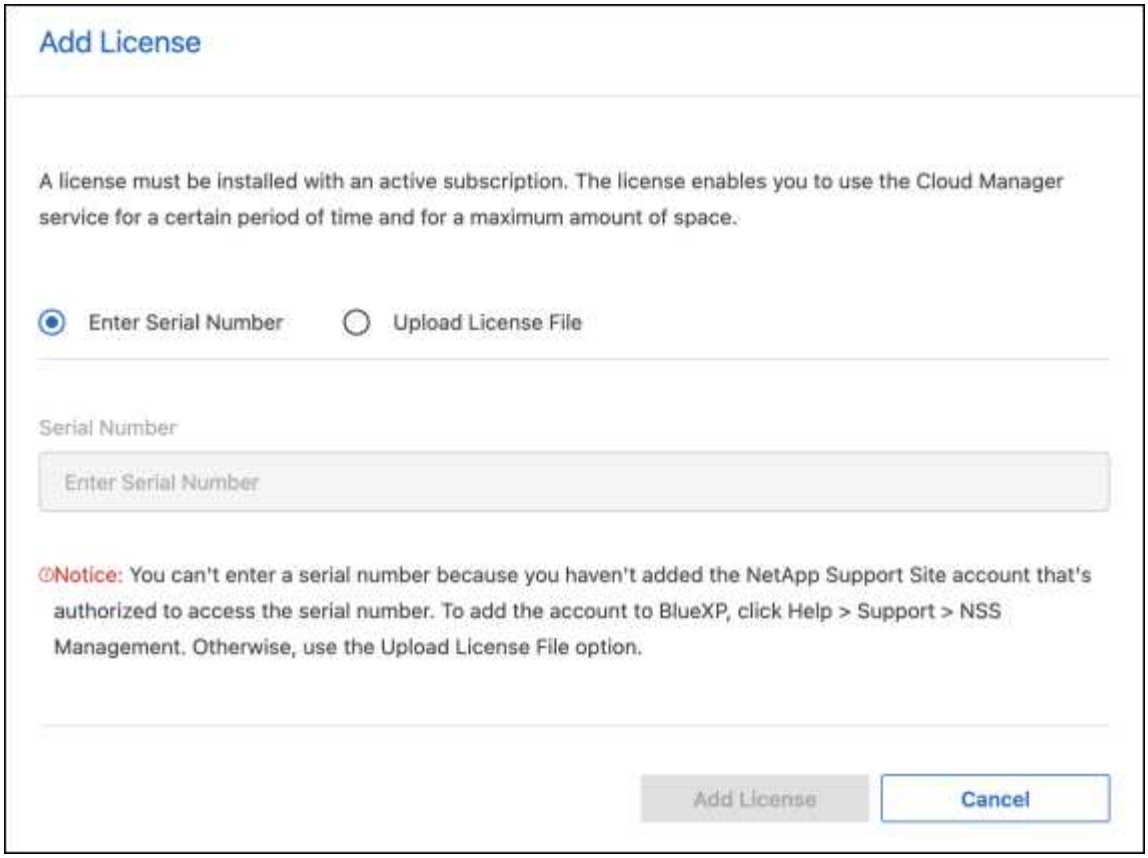
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página de Métodos de pago, seleccione **Suscribirse** a **Amazon Web Services**.
3. En AWS Marketplace, seleccione **Ver opciones de compra**.
4. Utilice AWS Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en AWS Marketplace.

6. Regresar a la página de métodos de pago de Ransomware Resilience.
7. Agregue la licencia a la Consola seleccionando **Agregar licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie**, ingrese el número de serie que se incluyó en el correo electrónico que le enviamos y luego seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia, desde la navegación izquierda de la Consola, seleccione **Administración** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

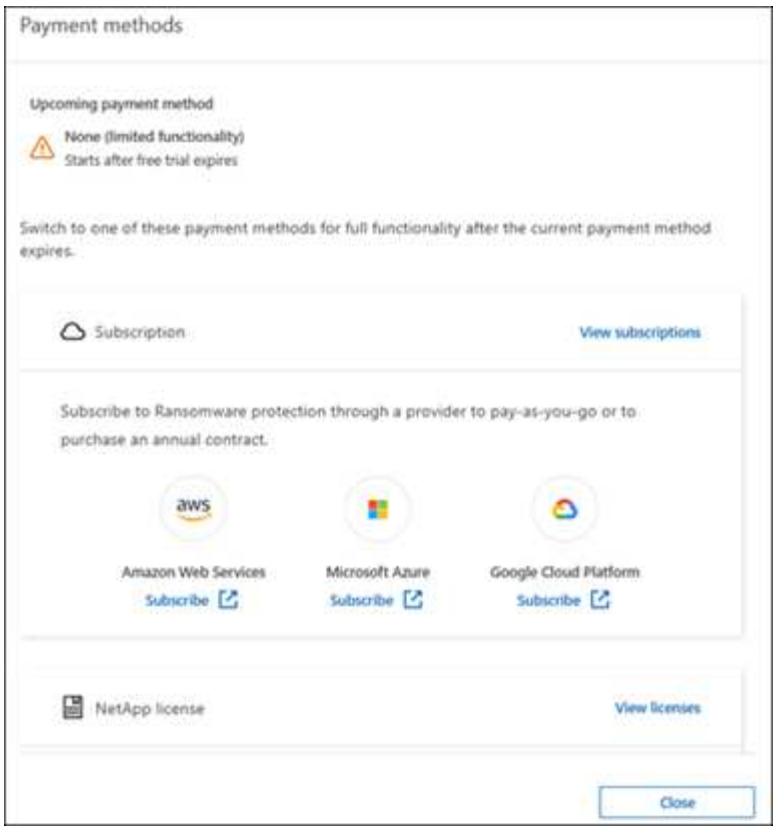
    Un mensaje confirma que se ha agregado una licencia.

Suscríbete a través de Microsoft Azure Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en Azure Marketplace.

Pasos

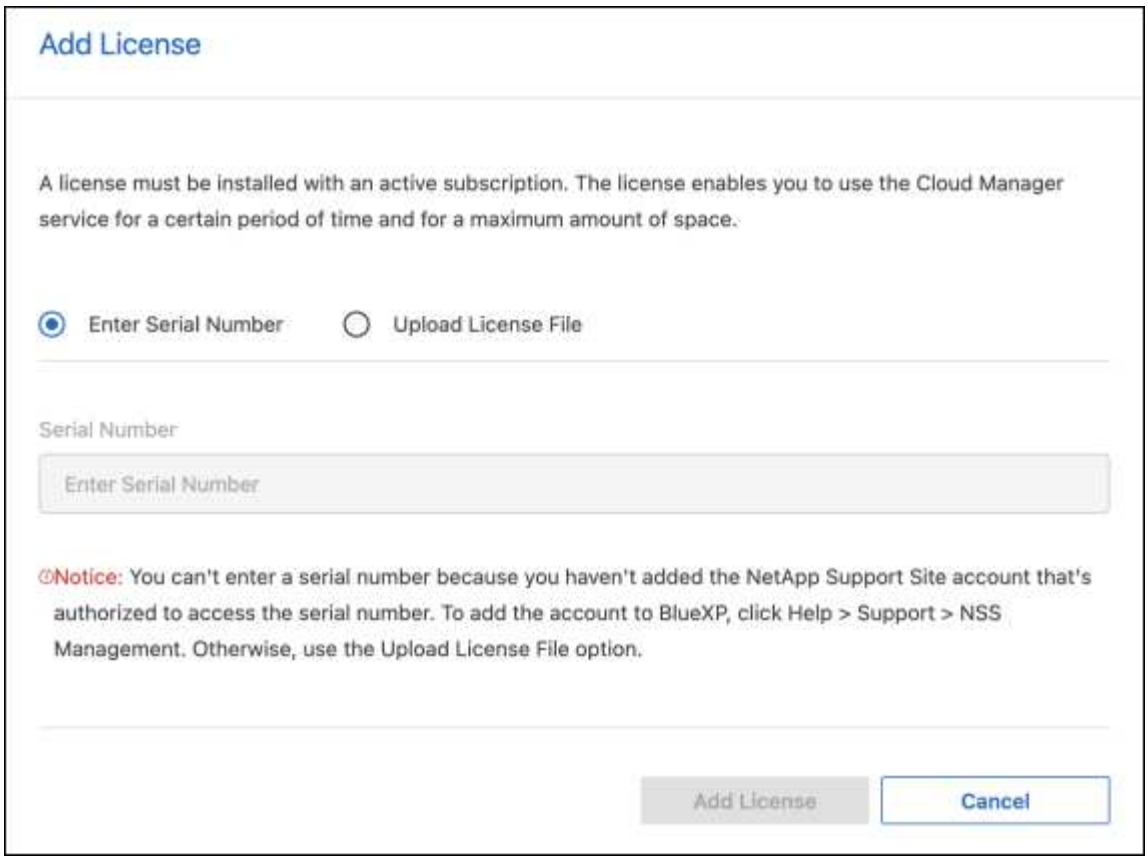
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página Métodos de pago, seleccione **Suscribirse** para **Microsoft Azure Marketplace**.
3. En Azure Marketplace, seleccione **Ver opciones de compra**.
4. Utilice Azure Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en Azure Marketplace.

6. Regresar a la página de Métodos de pago de Ransomware Resilience.
7. Para agregar la licencia, seleccione **Agregar una licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie** y luego ingrese el número de serie en el correo electrónico que le enviamos. Seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia en Licenses and subscriptions, desde la navegación izquierda de la Consola, seleccione **Gobernanza** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

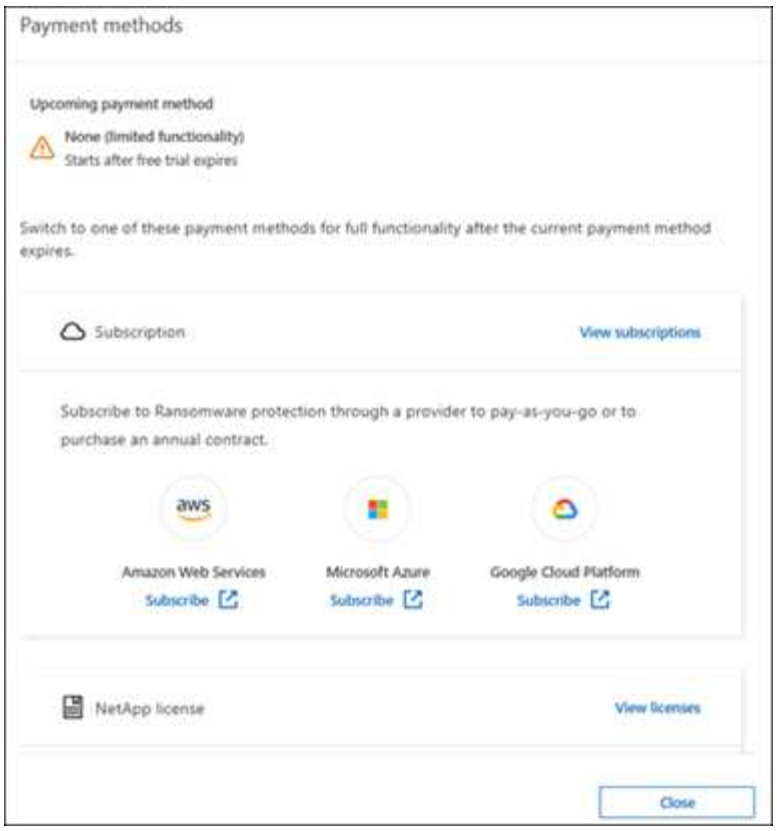
    Aparece un mensaje indicando que se ha añadido una licencia.

Suscríbete a través de Google Cloud Platform Marketplace

Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en Google Cloud Platform Marketplace.

Pasos

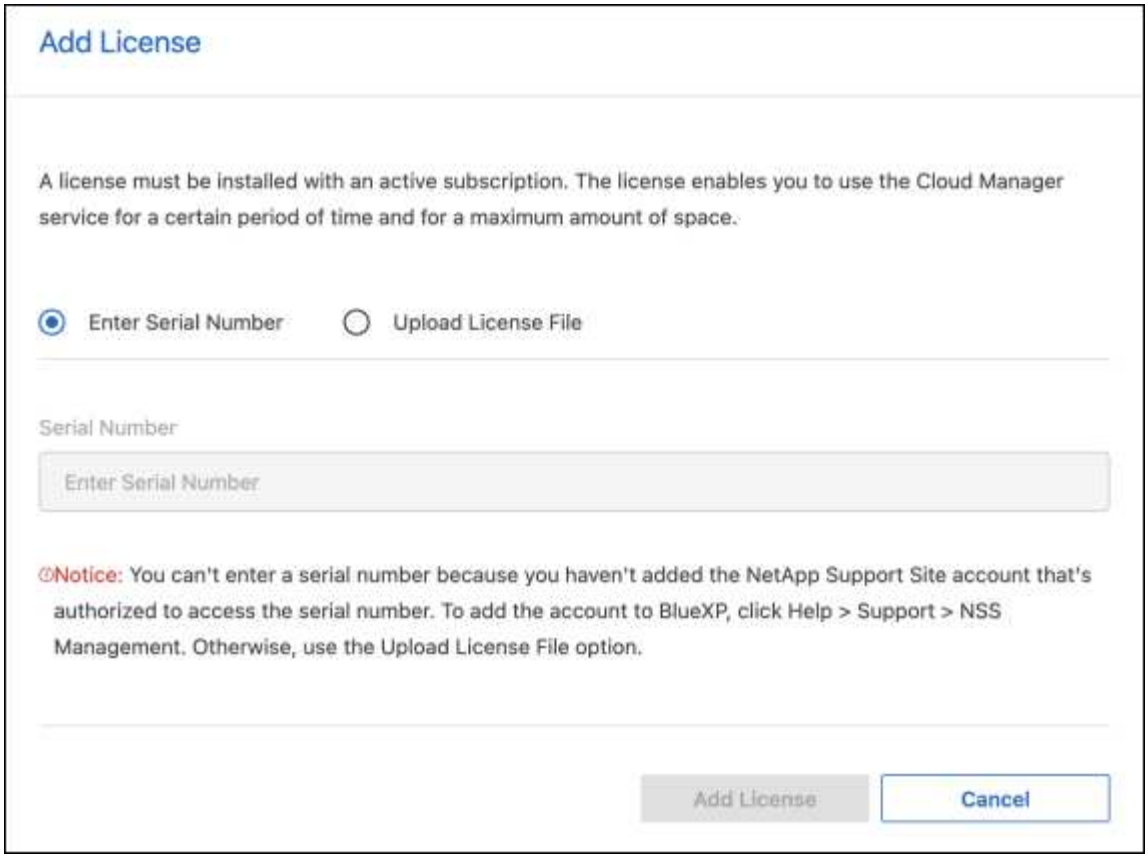
1. En Ransomware Resilience, realice una de las siguientes acciones:
   - Si aparece un mensaje que indica que la prueba gratuita está por vencer, seleccione **Ver métodos de pago**.
   - Si aún no ha comenzado la prueba, seleccione el aviso **Prueba gratuita** en la parte superior derecha y luego **Ver métodos de pago**.



2. En la página Métodos de pago, seleccione **Suscribirse** a Google Cloud Platform Marketplace*.
3. En Google Cloud Platform Marketplace, seleccione **Suscribirse**.
4. Utilice Google Cloud Platform Marketplace para suscribirse a * NetApp Intelligent Services* y * Ransomware Resilience *.
5. Cuando regresa a Ransomware Resilience, un mensaje indica que está suscrito.

> Se le envía un correo electrónico que incluye el número de serie de Ransomware Resilience e indica que Ransomware Resilience está suscrito en Google Cloud Platform Marketplace.

6. Regresar a la página de Métodos de pago de Ransomware Resilience.
7. Para agregar la licencia a la Consola, seleccione **Agregar licencia**.



8. En la página Agregar licencia, seleccione **Ingresar número de serie**. Introduzca el número de serie en el correo electrónico que le enviamos. Seleccione **Agregar licencia**.
9. Para ver los detalles de la licencia, desde la navegación izquierda de la Consola, seleccione **Gobernanza** > * Licenses and subscriptions*.
   - Para ver la información de la suscripción, seleccione **Suscripciones**.
   - Para ver las licencias BYOL, seleccione **Licencias de servicios de datos**.
10. Regresar a Resiliencia frente al ransomware. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Resiliencia ante ransomware**.

    Aparece un mensaje indicando que se ha añadido una licencia.

Traiga su propia licencia (BYOL)

Si desea traer su propia licencia (BYOL), debe comprar la licencia, obtener el archivo de licencia de NetApp (NLF) y luego agregar la licencia a la consola.

Agregue su archivo de licencia a la consola

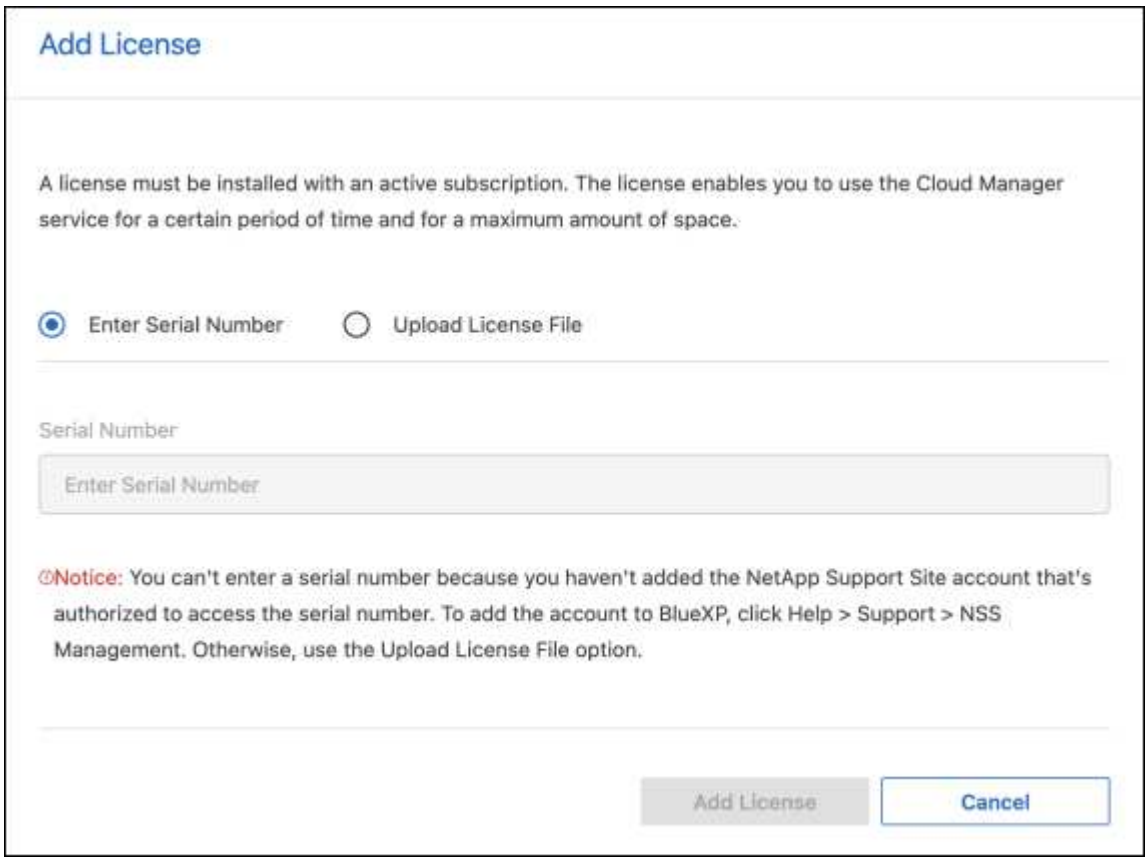
Una vez que haya comprado su licencia de Ransomware Resilience a su representante de ventas de NetApp , active la licencia ingresando el número de serie de Ransomware Resilience y la información de la cuenta del sitio de soporte de NetApp (NSS).

Antes de empezar

Necesita el número de serie de Ransomware Resilience. Localice este número en su orden de venta o comuníquese con el equipo de cuentas para obtener esta información.

Pasos

1. Después de obtener la licencia, regrese a Ransomware Resilience. Seleccione la opción **Ver métodos de pago** en la parte superior derecha. O bien, en el mensaje que indica que la prueba gratuita está por vencer, seleccione **Suscribirse o comprar una licencia**.
2. Seleccione **Agregar licencia** para ir a la página de Licencias y suscripciones de la consola.
3. Desde la pestaña **Licencias de servicios de datos**, seleccione **Agregar licencia**.



4. En la página Agregar licencia, ingrese el número de serie y la información de la cuenta del sitio de soporte de NetApp .
   - Si tiene el número de serie de la licencia de la consola y conoce su cuenta NSS, seleccione la opción **Ingresar número de serie** e ingrese esa información.

     Si su cuenta del sitio de soporte de NetApp no está disponible en la lista desplegable, "Agregue la cuenta NSS a la consola" .

   - Si tiene el archivo de licencia de zvondolr (necesario cuando se instala en un sitio oscuro), seleccione la opción **Cargar archivo de licencia** y siga las instrucciones para adjuntar el archivo.
5. Seleccione **Agregar licencia**.

Resultado

La página Licenses and subscriptions muestra que Ransomware Resilience tiene una licencia.

Actualice su licencia de consola cuando caduque

Si su período de licencia está cerca de la fecha de vencimiento, o si su capacidad de licencia está llegando al límite, se le notificará en la interfaz de usuario de resiliencia ante ransomware. Puede actualizar su licencia de

Ransomware Resilience antes de que expire para que no haya interrupciones en su capacidad de acceder a sus datos escaneados.

Este mensaje también aparece en Licenses and subscriptions y en "Configuración de notificaciones" .

Pasos

1. Puede enviar un correo electrónico al soporte para solicitar una actualización de su licencia.

   Una vez que paga la licencia y la registra en el sitio de soporte de NetApp , la consola actualiza automáticamente la licencia. La página de Licencias de Servicios de Datos reflejará el cambio en 5 a 10 minutos.

2. Si la consola no puede actualizar automáticamente la licencia, deberá cargar manualmente el archivo de licencia.
   a. Puede obtener el archivo de licencia en el sitio de soporte de NetApp .
   b. En la consola, seleccione **Administración** > **Licenses and subscriptions**.
   c. Seleccione la pestaña **Licencias de servicios de datos**, seleccione el ícono **Acciones…** para el número de serie que está actualizando y luego seleccione **Actualizar licencia**.

Finalizar la suscripción PAYGO

Si desea finalizar su suscripción PAYGO, puede hacerlo en cualquier momento.

Pasos

1. En Ransomware Resilience, en la parte superior derecha, seleccione la opción de licencia.
2. Seleccione **Ver métodos de pago**.
3. En los detalles desplegables, desmarque la casilla **Usar después de que expire el método de pago actual**.
4. Seleccione **Guardar**.

Más información

- "Documentación de licencias y suscripciones de NetApp Console"

Descubre las cargas de trabajo en NetApp Ransomware Resilience

Antes de poder utilizar NetApp Ransomware Resilience, primero debe descubrir los datos de la carga de trabajo. Durante el descubrimiento, Ransomware Resilience analiza todos los volúmenes y archivos de los sistemas en todos los agentes de la consola y proyectos dentro de una organización.

En el panel de Discovery, Ransomware Resilience muestra las configuraciones del sistema compatibles y no compatibles. Ransomware Resilience evalúa aplicaciones Oracle, almacenes de datos VMware, recursos compartidos de archivos y almacenamiento en bloques.

Ransomware Resilience no descubre cargas de trabajo con volúmenes que utilizan FlexGroup.

Ransomware Resilience comprueba tu protección actual de copias de seguridad, copias instantáneas y opciones de NetApp Autonomous Ransomware Protection. Ransomware Resilience también detecta información de protección de NetApp Backup and Recovery para file shares y VM file shares. Luego te recomienda maneras de mejorar tu protección contra ransomware.

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" .

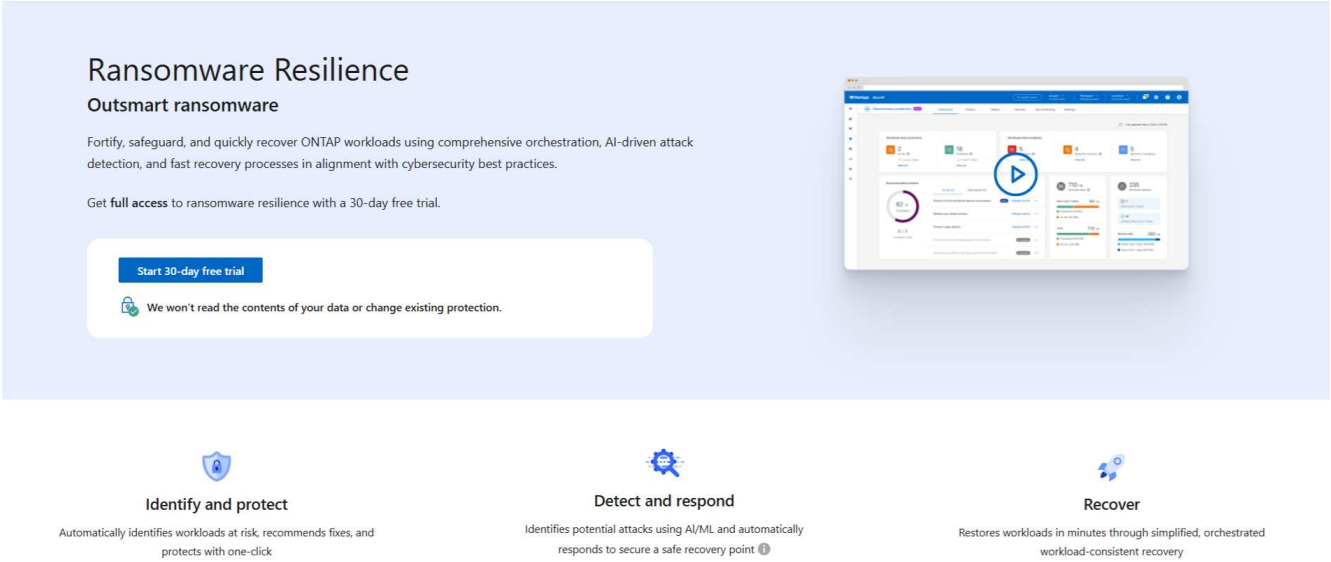
Seleccione cargas de trabajo para descubrir y proteger

Dentro de cada agente de consola, seleccione los sistemas en los que desea descubrir cargas de trabajo.

Pasos

1. Desde la NetApp Console, seleccione **Protección** > **Protección contra ransomware**.

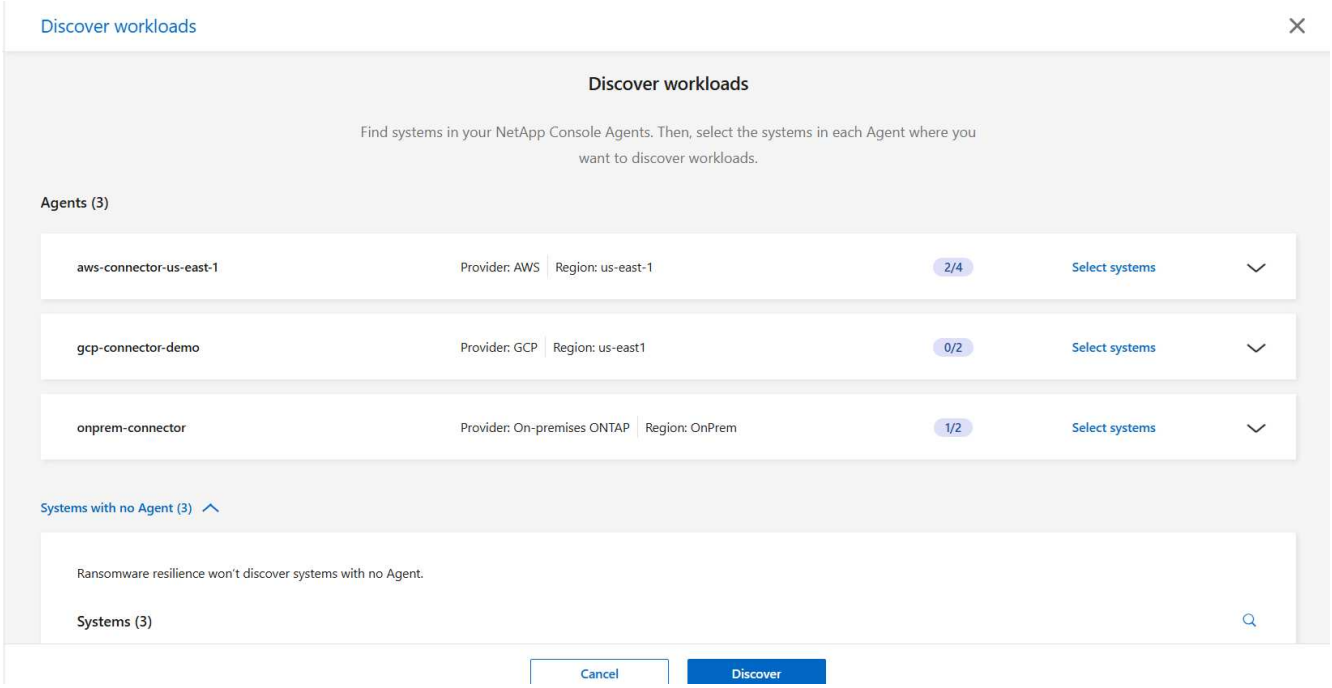
   Si este es su primer inicio de sesión, aparecerá la página de destino.



   Si inició la prueba gratuita, la etiqueta del botón **Iniciar prueba gratuita de 30 días** cambia a **Comenzar descubriendo cargas de trabajo**.

2. Desde la página de destino inicial, seleccione **Comenzar por descubrir cargas de trabajo**.

   Ransomware Resilience encuentra sistemas compatibles y no compatibles. Este proceso puede tardar unos minutos.

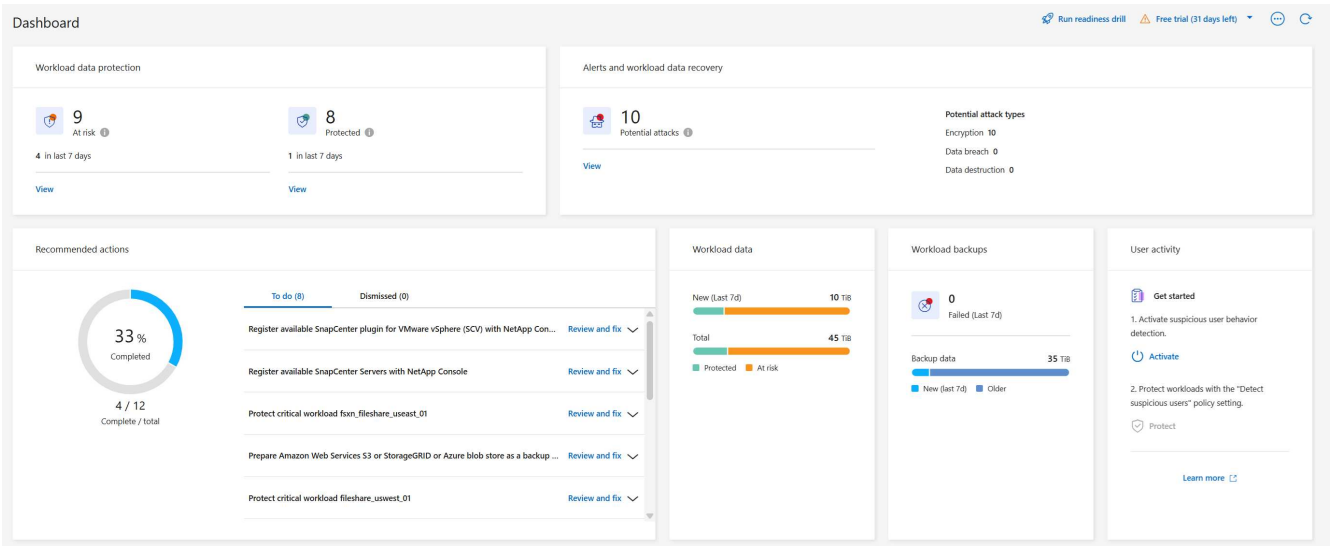


3. Para descubrir cargas de trabajo para un agente de consola específico, seleccione **Seleccionar sistemas** junto al agente de consola donde desea descubrir cargas de trabajo.
4. Seleccione los sistemas en los que desea descubrir cargas de trabajo.
5. Seleccione **Descubrir**.

   Ransomware Resilience solo descubre datos de carga de trabajo cuando selecciona el sistema. El proceso de descubrimiento puede tardar varios minutos.

6. Para descargar la lista de cargas de trabajo descubiertas, seleccione **Descargar resultados**.
7. Para mostrar el panel de resiliencia ante ransomware, seleccione **Ir al panel**.

   El panel muestra la salud de la protección de datos. El número de cargas de trabajo en riesgo o protegidas se actualiza a medida que se descubren nuevas cargas de trabajo.



"Aprende lo que te muestra el dashboard."

Descubra cargas de trabajo recién creadas para sistemas previamente seleccionados

Si agregó cargas de trabajo a un sistema descubierto previamente, deberá reiniciar la detección para proteger las nuevas cargas de trabajo.

Pasos

1. Para identificar la hora del último descubrimiento, observe la fecha y la hora junto al ícono **Actualizar** en la parte superior derecha del panel de resiliencia ante ransomware.
2. Desde el panel de control, selecciona el icono **Refresh** para encontrar nuevas cargas de trabajo.

Si encuentra que hay volúmenes que no se muestran para el sistema que descubrió, es posible que dichos volúmenes no sean compatibles. Para encontrar una lista de volúmenes no compatibles, vaya al menú **Configuración** y luego seleccione el menú de acciones en la tarjeta de descubrimiento de carga de trabajo para descargar un informe JSON de volúmenes compatibles y no compatibles.

Descubra nuevos sistemas

Si ya descubriste cargas de trabajo, puedes encontrar nuevas o aquellas que no seleccionaste antes.

Pasos

1. En Ransomware Resilience, selecciona **Configuración**.
2. En la tarjeta Descubrimiento de carga de trabajo, seleccione **Descubrir cargas de trabajo**. El descubrimiento puede tardar unos minutos. Un icono de carga muestra el progreso.
3. Ransomware Resilience descubre sistemas compatibles y no compatibles. No es compatible con un sistema si su versión de ONTAP es inferior a la versión requerida. Cuando pasa el cursor sobre un sistema no compatible, aparece una información sobre herramientas que muestra el motivo. Seleccione los sistemas en los que desea descubrir cargas de trabajo.
4. Seleccione **Descubrir**.

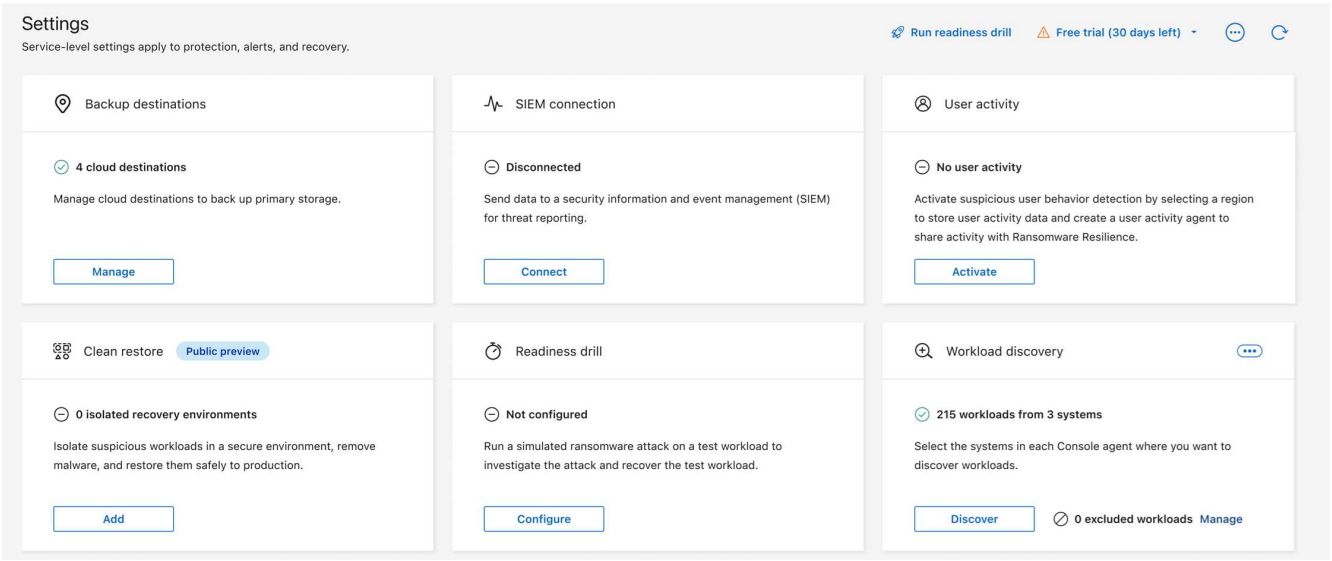
Excluir cargas de trabajo

Ransomware Resilience le permite excluir cargas de trabajo específicas en un sistema de la protección y detección de ransomware.

Solo puede excluir cargas de trabajo que sean compatibles y que se hayan detectado correctamente. Puede modificar la lista de cargas de trabajo excluidas en cualquier momento. No se le facturarán las cargas de trabajo excluidas de Ransomware Resilience.

Agregar cargas de trabajo a la lista de cargas de trabajo excluidas

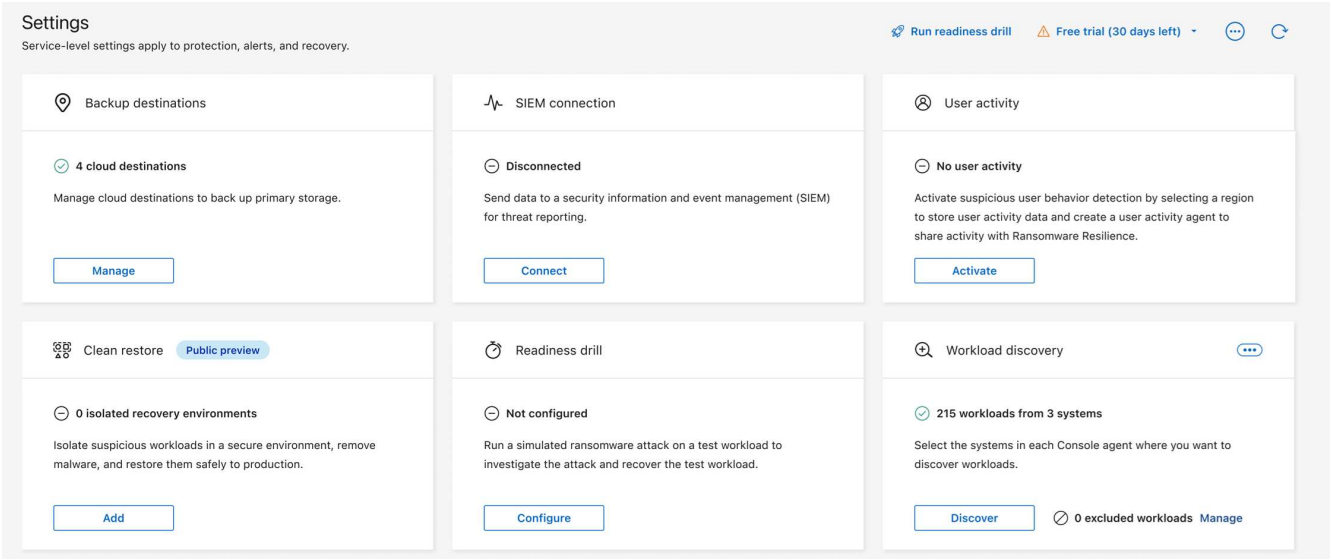
1. En Ransomware Resilience, seleccione **Configuración**.
2. En el panel de Configuración, busque el panel de Descubrimiento de carga de trabajo. La tarjeta identifica el número de cargas de trabajo excluidas. Para agregar cargas de trabajo, junto a las cargas de trabajo excluidas, seleccione **Administrar**.



3. En la página Cargas de trabajo excluidas, seleccione **Agregar**.
4. Seleccione las cargas de trabajo que desea excluir y luego **Agregar**.
5. Revise las cargas de trabajo excluidas en la página Cargas de trabajo excluidas. Mientras se agrega la carga de trabajo, se muestra un indicador de progreso junto a su nombre. Si una carga de trabajo no se excluyó correctamente, no se muestra en la página.

Eliminar cargas de trabajo de la lista de cargas de trabajo excluidas

1. En Ransomware Resilience, seleccione **Configuración**.
2. En el panel de Configuración, busque el panel de Descubrimiento de carga de trabajo. La tarjeta identifica el número de cargas de trabajo excluidas. Junto a las cargas de trabajo excluidas, seleccione **Administrar**.



3. Para eliminar una carga de trabajo individual, seleccione el menú de acciones de la carga de trabajo que desea eliminar de la lista de excluidos.

   Para eliminar varias cargas de trabajo, seleccione la casilla de verificación junto a las cargas de trabajo que desea eliminar y luego **Eliminar de excluidos**.

4. En el cuadro de diálogo, seleccione **Eliminar** para confirmar que desea eliminar las cargas de trabajo de la lista de exclusión.
5. Si la carga de trabajo se elimina de la lista de cargas de trabajo excluidas con éxito, aparece un mensaje de éxito en la página Carga de trabajo excluida y la carga de trabajo ya no aparece en la lista de cargas de trabajo excluidas. Si la acción falla, aparece un mensaje de error; intente la operación nuevamente.