Manos a la obra

BlueXP ransomware protection

NetApp
March 22, 2024

Tabla de contenidos

Manos a la obra

Obtén más información sobre la versión previa de la protección frente al ransomware de BlueXP

Los ataques de ransomware pueden bloquear el acceso a tus sistemas y los datos, y los atacantes pueden solicitar un rescate a cambio de la liberación de datos o descifrado. Según IDC, no es raro que las víctimas de ransomware sufran múltiples ataques de ransomware. El ataque puede interrumpir el acceso a los datos entre un día y varias semanas.

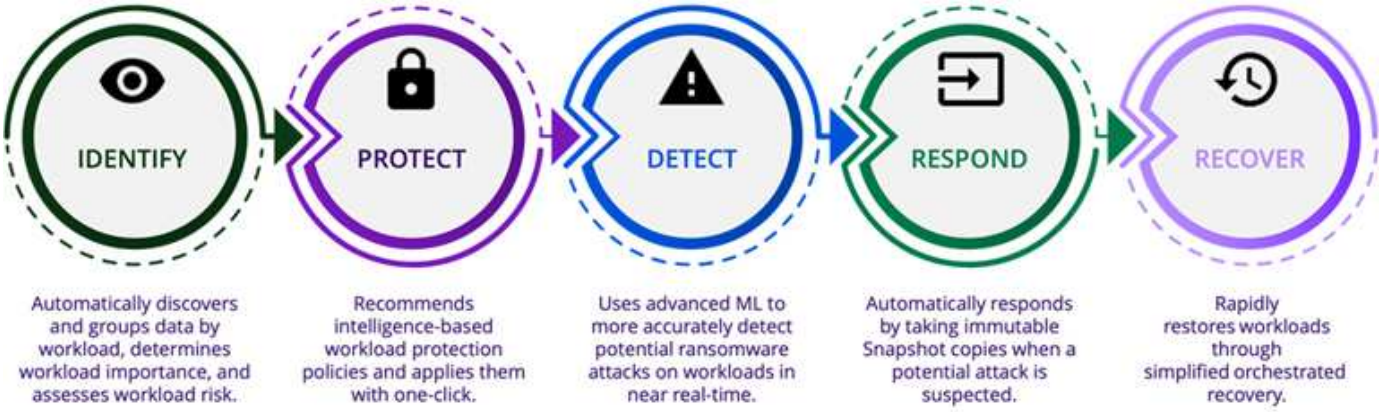
La protección frente al ransomware de BlueXP es un servicio de orquestación para la protección, detección y recuperación de ransomware. Para la versión de vista previa, el servicio protege las cargas de trabajo basadas en aplicaciones de Oracle, MySQL, almacenes de datos de máquinas virtuales, también se pueden compartir archivos en el almacenamiento NAS en las instalaciones, así como en Cloud Volumes ONTAP en Amazon Web Services (mediante el protocolo NFS) en cuentas de BlueXP y se realizan backups de los datos en el almacenamiento en cloud de Amazon Web Services o en NetApp StorageGRID.

ESTA DOCUMENTACIÓN SE PROPORCIONA COMO UNA PREVISUALIZACIÓN TECNOLÓGICA. Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y la línea de tiempo de la oferta antes de la disponibilidad general.

Todo lo que puedes hacer con la protección frente al ransomware de BlueXP

El servicio de protección frente a ransomware de BlueXP proporciona un uso completo de diversas tecnologías de NetApp para que el administrador de almacenamiento, el administrador de seguridad de los datos o el ingeniero de operaciones de seguridad puedan lograr los siguientes objetivos:

- **Identifica** todas las cargas de trabajo basadas en aplicaciones, de uso compartido o gestionadas por VMware en el NAS on-premises de NetApp con entornos de trabajo NFS en BlueXP, en cuentas de BlueXP, espacios de trabajo y conectores BlueXP. A continuación, el servicio categoriza la prioridad de los datos y te ofrece recomendaciones para llevar a cabo mejoras en la protección frente a ransomware.
- **Proteja** sus cargas de trabajo habilitando copias de seguridad y copias snapshot en sus datos.
- **Detectar** anomalías que podrían ser ataques de ransomware.
- * Responder* a posibles ataques de ransomware iniciando automáticamente una copia snapshot de NetApp ONTAP.
- * Recuperar* 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 optar por recuperar volúmenes, carpetas o archivos específicos. El servicio ofrece recomendaciones sobre las mejores opciones.



Beneficios de usar la protección frente al ransomware de BlueXP

La protección frente al ransomware de BlueXP ofrece las siguientes ventajas:

- Detecta las cargas de trabajo y los conjuntos de datos, analiza la prioridad en función del índice de uso y clasifica su importancia relativa.
- Evalúa tu posición de protección frente al ransomware y lo muestra en una consola fácil de entender.
- Proporciona recomendaciones sobre los siguientes pasos según el análisis de la postura de detección y protección.
- Aplica recomendaciones de protección de datos impulsadas por IA/ML con acceso con un solo clic.
- Protege los datos en las principales cargas de trabajo basadas en aplicaciones, como MySQL, Oracle, almacenes de datos de VMware y recursos compartidos de archivos.
- Detecta ataques de ransomware en datos en tiempo real en almacenamiento principal mediante tecnología de IA.
- Inicia acciones automatizadas en respuesta a posibles ataques detectados creando copias Snapshot e iniciando alertas sobre actividad anormal.
- Aplica una recuperación selectiva para cumplir con las políticas del objetivo de punto de recuperación. La protección contra ransomware de BlueXP orquesta la recuperación de incidentes de ransomware mediante diversos servicios de recuperación de NetApp, incluidos el backup y la recuperación de datos de BlueXP (anteriormente Cloud Backup).

Coste

NetApp no te cobra por usar la versión preliminar de la protección contra ransomware de BlueXP.

Licencia

La versión previa de la protección contra ransomware de BlueXP no requiere ninguna licencia especial. Todas las licencias de vista previa son licencias de evaluación.

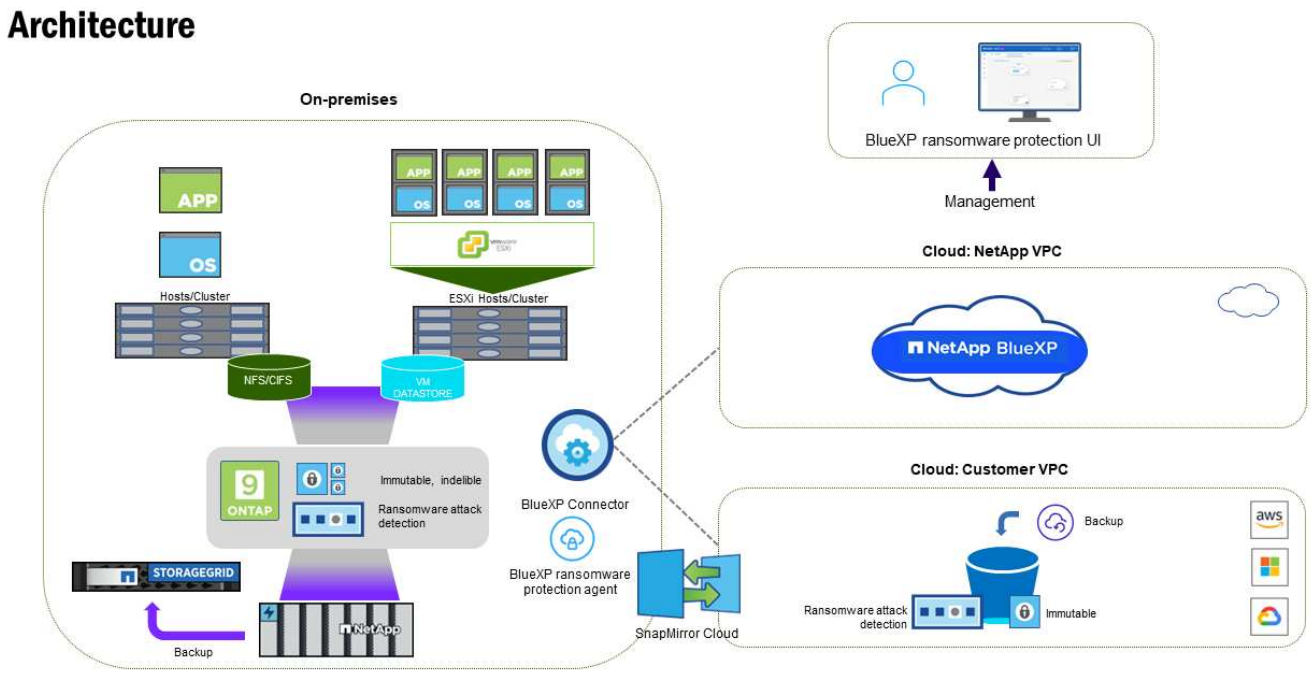
Para la versión de vista previa, NetApp ayuda a configurar la evaluación y las licencias necesarias.

La vista previa de la protección contra ransomware de BlueXP requiere las siguientes licencias:

- ONTAP
- Tecnología autónoma de protección frente a ransomware de NetApp. Consulte "Información general sobre la protección de ransomware autónoma" para obtener más detalles.
- Servicio de backup y recuperación de datos de BlueXP

Funcionamiento de la protección frente al ransomware de BlueXP

En un nivel alto, la protección contra el ransomware de BlueXP funciona así.



Función	Descripción
IDENTIFICAR	• Encuentra todos los datos de NAS (montajes NFS) en las instalaciones de los clientes conectados a BlueXP. • Identifica los datos de los clientes de las API de servicios de ONTAP y los asocia con las cargas de trabajo. Más información acerca de "ONTAP" y.. "Software SnapCenter". • Detecta el nivel de protección actual de cada volumen de copias de Snapshot de NetApp y políticas de backup, así como cualquier funcionalidad de detección integrada. A continuación, el servicio asocia esta postura de protección con las cargas de trabajo mediante el backup y recuperación de datos de BlueXP, el asesor digital de BlueXP, los servicios de ONTAP y tecnologías de NetApp como la protección autónoma frente a ransomware, FPolicy, las políticas de backup y las políticas de Snapshot. Más información acerca de "Protección autónoma de ransomware" y.. "Backup y recuperación de BlueXP", "Asesor digital de BlueXP", y. "FPolicy de ONTAP". • Asigna una prioridad empresarial a cada carga de trabajo en función de los niveles de protección detectados automáticamente y recomienda políticas de protección para las cargas de trabajo en función de su prioridad empresarial. • La protección frente al ransomware también aprende las asociaciones de políticas y recomienda tus políticas personalizadas en cargas de trabajo similares.
PROTEGER	• Supervisa activamente las cargas de trabajo y orquesta el uso de las API de backup y recuperación de datos de BlueXP y ONTAP mediante la aplicación de políticas a cada una de las cargas de trabajo identificadas.
DETECTAR	• Detecta posibles ataques 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 la respuesta a actividades anormales realizando copias Snapshot adicionales automatizadas para crear los puntos de restauración de datos más cercanos. El servicio ofrece la capacidad de obtener más información para identificar posibles ataques con mayor precisión sin que ello afecte al rendimiento de las cargas de trabajo principales. • Determina los archivos y mapas sospechosos específicos que atacan a las cargas de trabajo asociadas mediante las tecnologías ONTAP, protección autónoma contra ransomware y FPolicy.
RESPONDER	• Muestra datos relevantes, como la actividad de los archivos, la actividad del usuario y la entropía, para ayudarte a realizar revisiones forenses sobre el ataque. • Inicia rápidas copias Snapshot usando tecnologías y productos de NetApp como ONTAP, protección autónoma frente a ransomware y FPolicy.

Función	Descripción
RECUPERAR	• Determina la mejor copia Snapshot o backup y recomienda el mejor punto de recuperación real (RPA) mediante el uso de las tecnologías y servicios de backup y recuperación de datos de BlueXP, ONTAP, protección autónoma frente a ransomware y FPolicy. • Orquesta la recuperación de cargas de trabajo que incluyen máquinas virtuales, recursos compartidos de archivos y bases de datos con coherencia de aplicaciones.

Destinos de copia de seguridad, entornos de trabajo y orígenes de datos compatibles

Utiliza la vista previa de la protección de ransomware de BlueXP para ver lo resilientes que son tus datos ante un ciberataque a los siguientes tipos de destinos de backup, entornos de trabajo y fuentes de datos:

Destinos de copia de seguridad soportados

- Amazon Web Services (AWS) S3
- StorageGRID de NetApp
- Entornos de trabajo compatibles *
- NAS de ONTAP en las instalaciones (con el protocolo NFS)
- ONTAP Select
- Cloud Volumes ONTAP en AWS (con el protocolo NFS)

Fuentes de datos

Para la versión de vista previa, el servicio protege las siguientes cargas de trabajo basadas en aplicaciones:

- Recursos compartidos de archivos NetApp
- Almacenes de datos VMware
- Bases de datos (para la versión preliminar, Oracle y MySQL)

Términos que pueden ayudarte con la protección contra el ransomware

Te puedes beneficiar si comprendes alguna terminología en lo que respecta a la protección contra ransomware.

- **Protección**: La protección en la protección contra ransomware de BlueXP significa garantizar que las copias Snapshot y las copias de seguridad inmutables se produzcan de forma regular en un dominio de seguridad diferente mediante políticas de protección.
- **Carga de trabajo**: Una carga de trabajo en la vista previa de protección contra ransomware de BlueXP puede incluir bases de datos MySQL u Oracle, almacenes de datos de VMware o recursos compartidos de archivos.

Requisitos previos de protección contra ransomware de BlueXP

Comience a usar la protección frente al ransomware de BlueXP verificando la preparación de su entorno operativo, inicio de sesión, acceso a red y navegador web.

Para utilizar la versión previa de la protección contra ransomware de BlueXP, necesitarás estos requisitos previos:

- Una cuenta en NetApp StorageGRID o AWS S3 para los destinos de backup y los permisos de acceso establecidos

  Consulte la "Lista de permisos de AWS" para obtener más detalles.

- ONTAP 9.11.1 y versiones posteriores
  - Permisos de la ONTAP del administrador de clústeres
  - Una licencia de la protección autónoma frente a ransomware de NetApp, utilizada por la protección frente a ransomware de BlueXP, habilitada en la instancia de ONTAP en las instalaciones, según la versión de ONTAP que esté utilizando. Consulte "Información general sobre la protección de ransomware autónoma".

    Para obtener más información sobre las licencias, consulte "Obtén más información sobre la protección frente al ransomware de BlueXP".

- En BlueXP:
  - Debe configurarse un conector BlueXP por cada cloud privado virtual (VPC) o en una región en las instalaciones en BlueXP. Consulte "Documentación de BlueXP para configurar el Connector".

    > Si tienes varios BlueXP Connectors, el servicio analizará los datos en todos los conectores más allá de los que se muestren actualmente en la interfaz de usuario de BlueXP.

  - El servicio de backup y recuperación de BlueXP con backup habilitado en el entorno de trabajo
  - Un entorno de trabajo BlueXP con almacenamiento on-premises NAS de NetApp
  - Una cuenta de BlueXP con al menos un conector activo que se conecta a clústeres de ONTAP en las instalaciones. Todos los entornos de trabajo y origen deben estar en la misma cuenta de BlueXP.
  - Una cuenta de usuario de BlueXP con privilegios de administrador de cuenta para detectar recursos
  - "Requisitos estándar de BlueXP"

Inicio rápido para la protección frente al ransomware de BlueXP

Aquí tienes una descripción general de los pasos necesarios para empezar a utilizar la protección contra ransomware de BlueXP. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

Revise los requisitos previos

"Asegúrese de que su entorno cumpla estos requisitos".

Configura el servicio de protección contra ransomware

- "Preparar NetApp StorageGRID o Amazon Web Services como destino de backup".
- "Configura un conector en BlueXP".
- "Configurar destinos de copia de seguridad".
- "Detecta cargas de trabajo en BlueXP".

El futuro

Después de configurar el servicio, esto es lo que puede hacer a continuación.

- "Ver el estado de la protección de las cargas de trabajo en la consola".
- "Proteja las cargas de trabajo".
- "Responde a la detección de posibles ataques de ransomware".
- "Recuperarse de un ataque (después de neutralizar los incidentes)".

Configura la protección contra el ransomware de BlueXP

Para utilizar la protección contra ransomware de BlueXP, sigue algunos pasos para configurarla.

Antes de comenzar, revise "requisitos previos" garantizar que su entorno está listo.

Preparar el destino de la copia de seguridad

Prepare uno de los siguientes destinos de copia de seguridad:

- StorageGRID de NetApp
- Amazon Web Services

Después de configurar las opciones en el destino de backup, lo configurarás más adelante como destino de backup en el servicio de protección contra ransomware de BlueXP.

Preparar StorageGRID para que se convierta en destino de backup

Si desea usar StorageGRID como destino de backup, consulte "Documentación de StorageGRID" Para obtener más detalles acerca de StorageGRID.

Prepare AWS para que se convierta en destino de backup

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

Para obtener más información sobre la gestión de su almacenamiento de AWS en BlueXP, consulte "Gestione sus bloques de Amazon S3".

Configure BlueXP

El siguiente paso es configurar BlueXP y el servicio de protección contra ransomware de BlueXP.

Revisar "Requisitos estándar de BlueXP".

Crear un conector en BlueXP

Debe ponerse en contacto con su representante de ventas de NetApp para probar este servicio. Una vez que uses BlueXP Connector, incluirá las funcionalidades adecuadas para el servicio de protección frente a ransomware.

Para crear un conector en BlueXP antes de utilizar el servicio, consulte la documentación de BlueXP que se describe "Cómo crear un conector BlueXP".

> Si tienes varios BlueXP Connectors, el servicio analizará los datos en todos los conectores más allá de los que se muestren actualmente en la interfaz de usuario de BlueXP. Este servicio detecta todos los espacios de trabajo y todos los conectores asociados a esta cuenta.

Accede a la protección frente al ransomware de BlueXP

Utilizarás NetApp BlueXP para iniciar sesión en el servicio de protección contra ransomware de BlueXP. En la navegación izquierda de BlueXP, selecciona **Protección** > **Protección contra ransomware**.

Para obtener más información, consulte "Accede a la protección frente al ransomware de BlueXP".

Configura los destinos de backup en la protección frente al ransomware de BlueXP

Utiliza la opción de destinos de backup de protección contra ransomware de BlueXP para configurar destinos de backup. Para obtener más información, consulte "Configure las opciones de configuración".

Accede a la protección frente al ransomware de BlueXP

Utilizarás NetApp BlueXP para iniciar sesión en el servicio de protección contra ransomware de BlueXP.

Para iniciar sesión en BlueXP, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en cloud de NetApp con su correo electrónico y una contraseña. "Obtenga más información sobre cómo iniciar sesión".

Pasos

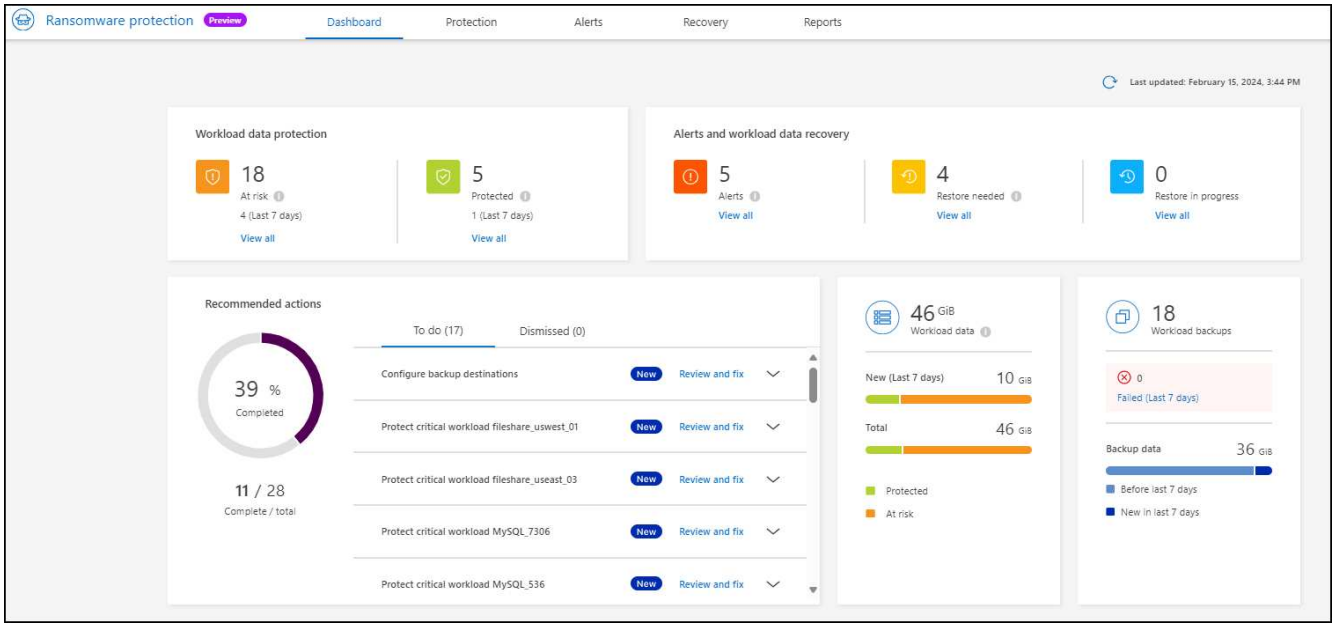
1. Abra un explorador web y vaya al "Consola BlueXP".

   Aparece la página de inicio de sesión de NetApp BlueXP.

2. Inicie sesión en BlueXP.
3. En la navegación izquierda de BlueXP, selecciona **Protección** > **Protección contra ransomware**.

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

De lo contrario, se mostrará la consola de protección contra ransomware de BlueXP.



4. Comience a utilizar el servicio.
   - Si no tienes un conector BlueXP o no es el indicado para esta vista previa, es posible que debas ponerte en contacto con el Soporte de NetApp o seguir mensajes para registrarte en esta vista previa.
   - Si eres nuevo en BlueXP y no has usado ningún conector, cuando seleccionas «**Protección contra ransomware**», aparecerá un mensaje sobre la inscripción. Continúe y envíe el formulario. NetApp se pondrá en contacto con usted para informarse sobre su solicitud de evaluación.
   - Si eres un usuario de BlueXP con un conector existente, cuando seleccionas «**Protección contra ransomware**», aparecerá un mensaje sobre la inscripción.
   - Si ya estás participando en la vista previa, al seleccionar "**Protección contra ransomware**", puedes continuar con el servicio. Si aún no lo ha hecho, debe seleccionar la opción **Descubrir cargas de trabajo**.

Detecta cargas de trabajo en la protección frente al ransomware de BlueXP

Para utilizar la protección frente al ransomware de BlueXP, el servicio debe detectar primero los datos. Durante la detección, la protección frente al ransomware de BlueXP analiza todos los volúmenes y archivos en entornos de trabajo en todos los conectores y espacios de trabajo de BlueXP dentro de una cuenta.

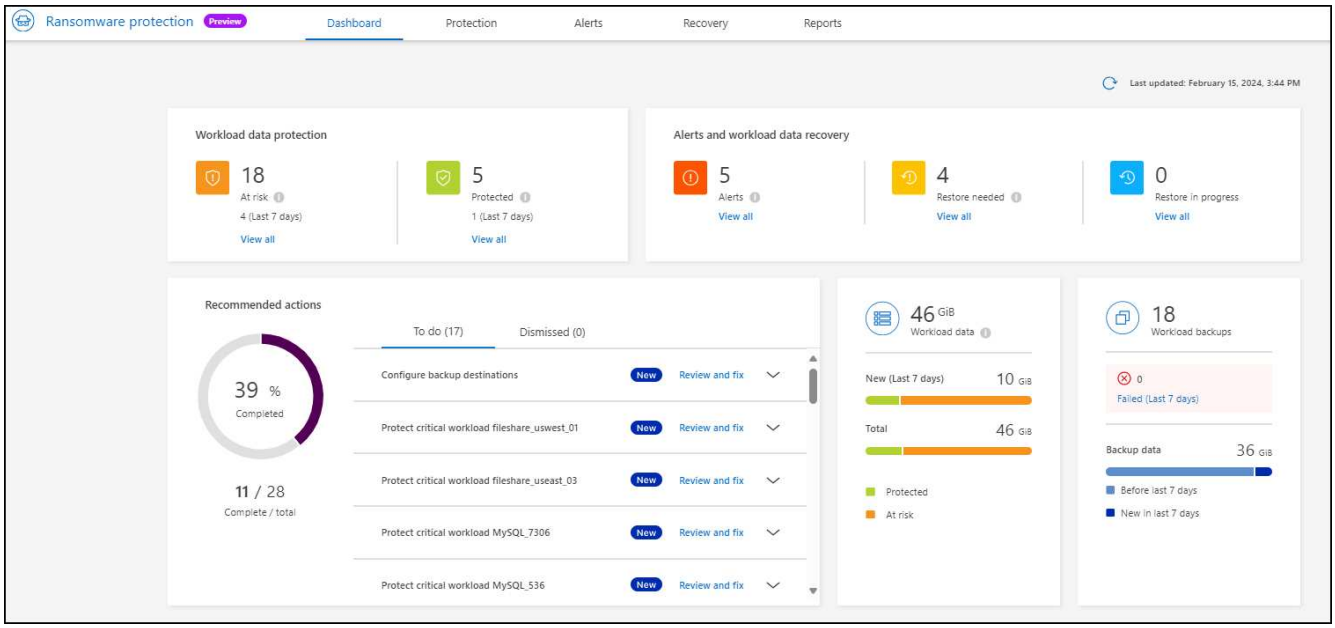
Para la versión preliminar, la protección frente al ransomware BlueXP evalúa las aplicaciones MySQL, las aplicaciones de Oracle, los almacenes de datos de VMware y los recursos compartidos de archivos.

El servicio evalúa el nivel de protección existente, incluida la protección actual del backup, las copias Snapshot y las opciones de protección autónoma frente a ransomware de NetApp. Según la evaluación, el servicio te recomienda cómo mejorar tu protección frente al ransomware.

Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección** > **Protección contra ransomware**.
2. Seleccione **Descubrir cargas de trabajo** en la página de destino inicial.

   El servicio detecta los datos de la carga de trabajo y muestra el estado de la protección de datos en la consola.



Configura las opciones de protección contra ransomware de BlueXP

Si desea configurar un destino de backup, revise las recomendaciones en la consola.

Agregue un destino de copia de seguridad

La protección frente al ransomware de BlueXP puede identificar cargas de trabajo que aún no tienen backups y también cargas de trabajo que todavía no tengan destinos de backup asignados.

Para proteger esas cargas de trabajo, debe añadir un destino de backup. Es posible elegir uno de los siguientes destinos de backup:

- StorageGRID de NetApp
- Amazon Web Services (AWS)

Puede añadir un destino de backup en función de una acción recomendada en la consola.

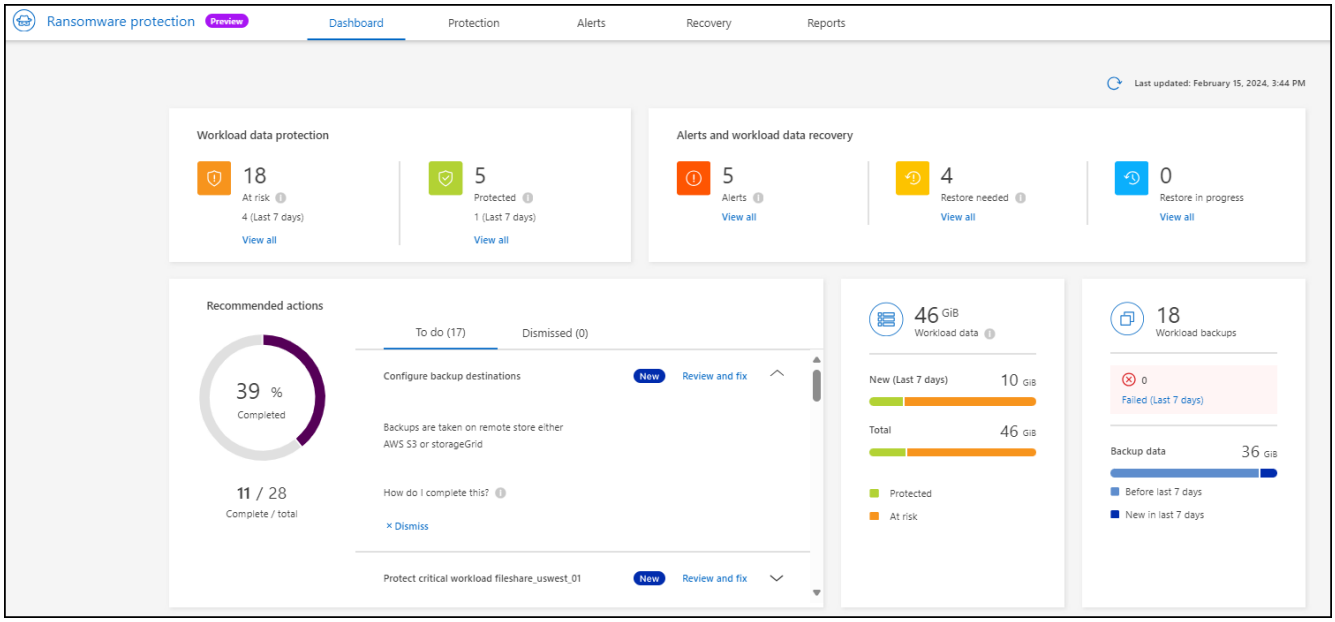
Acceda a las opciones de destino de copia de seguridad desde las acciones recomendadas del panel de control

La consola ofrece muchas recomendaciones. Una recomendación podría ser configurar un destino de copia de seguridad.

Pasos

1. En la navegación izquierda de BlueXP, selecciona **Protección** > **Protección contra ransomware**.

2. Revise el panel de acciones recomendadas de la consola.

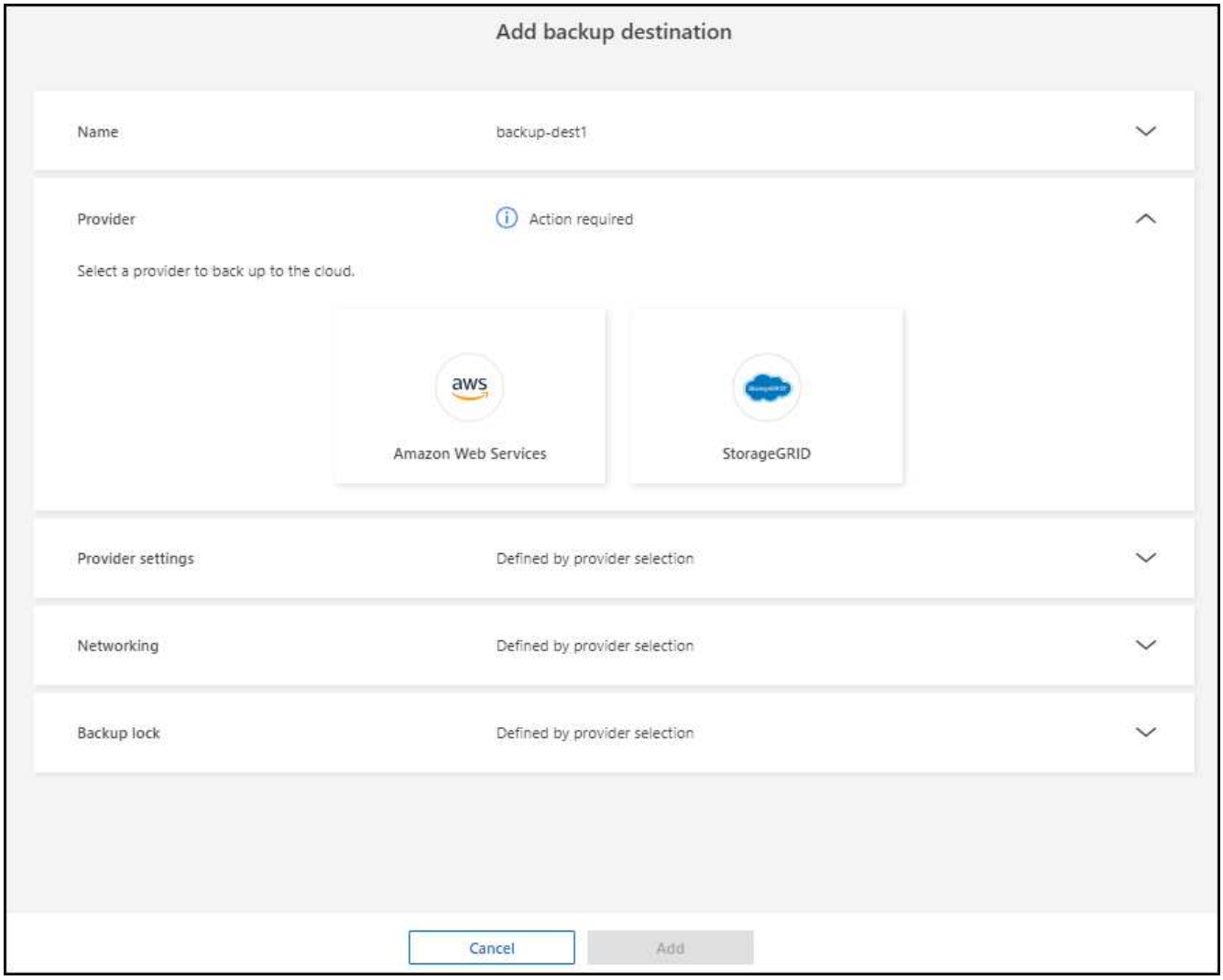


3. Desde el Panel de Control, seleccione **Revisar y corregir** para la recomendación de “Configurar destinos de copia de seguridad”.
4. Continúe con las instrucciones dependiendo del proveedor de copias de seguridad.

Añada StorageGRID como destino de backup

Para configurar NetApp StorageGRID como destino de backup, introduzca la siguiente información.

1. En la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.



3. Seleccione **StorageGRID**.
4. Seleccione la flecha hacia abajo junto a cada ajuste e introduzca o seleccione valores:
   - **Configuración del proveedor**:
     - Cree un nuevo bloque o traiga su propio bloque que almacenará los backups.
     - Nodo de puerta de enlace StorageGRID Nombre de dominio completo, puerto, clave de acceso a StorageGRID y credenciales de clave secreta.
   - **Networking**: Elige el espacio IP.
     - El espacio IP es el clúster donde residen los volúmenes del que se desea incluir en un backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.
   - * Bloqueo de respaldo*: Elija si desea que el servicio proteja las copias de seguridad de ser modificadas o eliminadas. Esta opción utiliza la tecnología DataLock de NetApp. Cada copia de seguridad se bloqueará durante el período de retención, o durante un mínimo de 30 días, más un período de búfer de hasta 14 días.

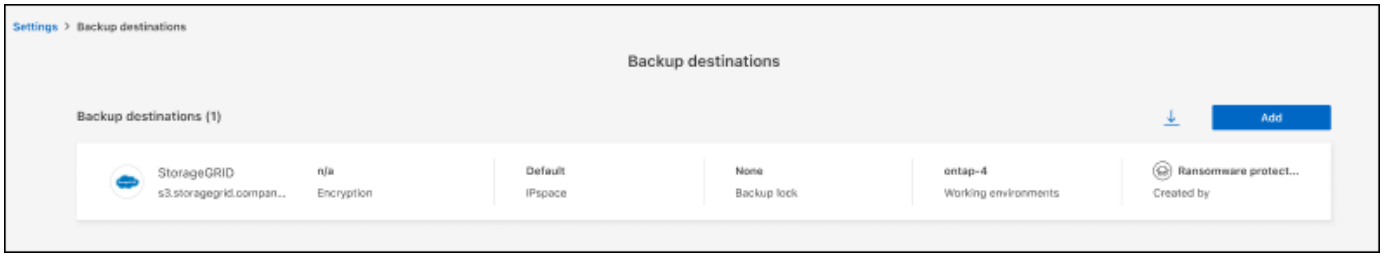
     Si configura ahora el ajuste de bloqueo de copia de seguridad, no es posible cambiarlo más tarde después de configurar el destino de copia de seguridad.

     - **Modo de cumplimiento**: Los usuarios no pueden sobrescribir ni eliminar los archivos de copia de seguridad protegidos durante el período de retención.

5. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.

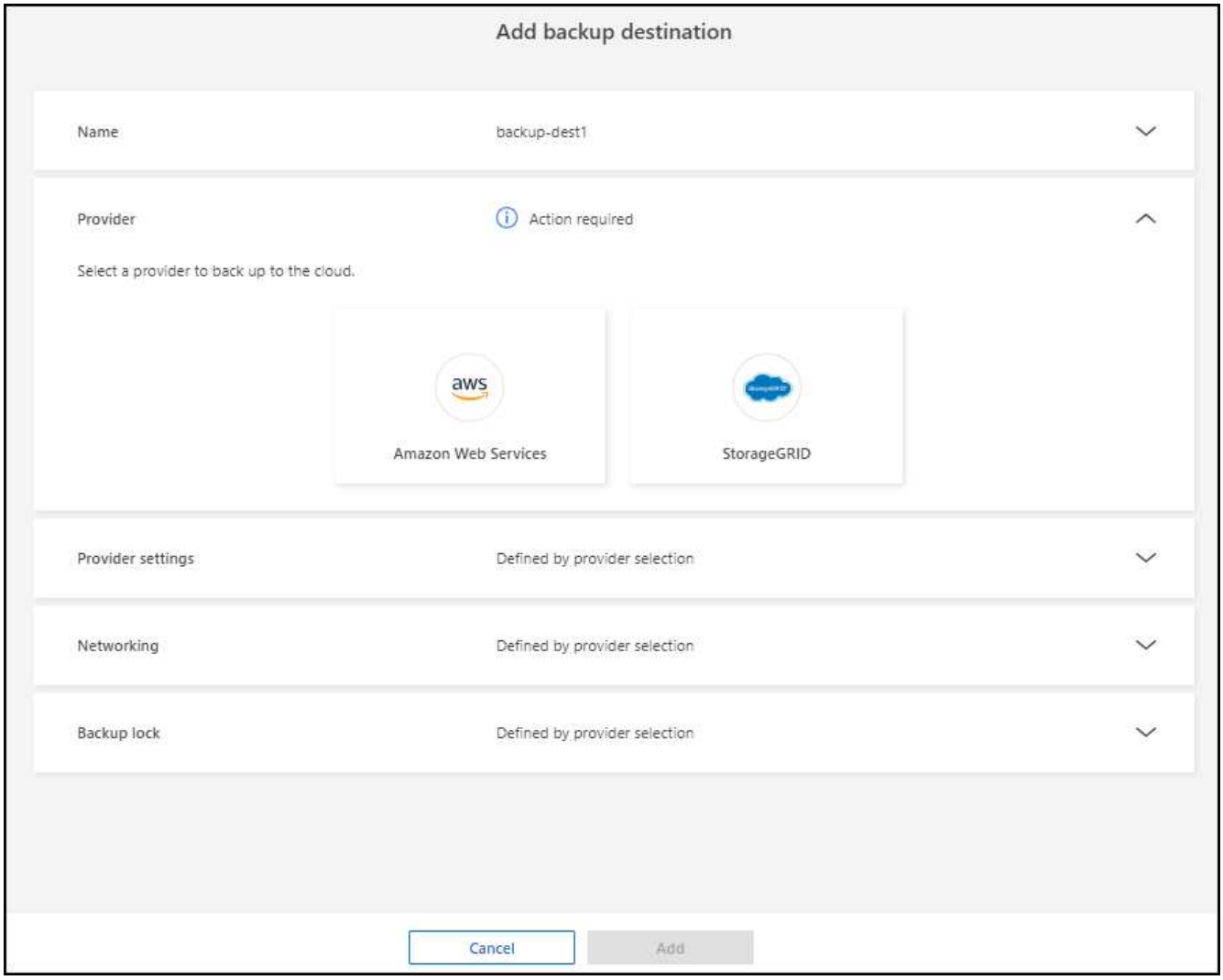


Añada Amazon Web Services como destino de backup

Para configurar AWS como destino de backup, introduzca la siguiente información.

Para obtener más información sobre la gestión de su almacenamiento de AWS en BlueXP, consulte "Gestione sus bloques de Amazon S3".

1. En la página **Configuración > Destinos de copia de seguridad**, seleccione **Agregar**.
2. Introduzca un nombre para el destino de la copia de seguridad.



3. Seleccione **Amazon Web Services**.
4. Seleccione la flecha hacia abajo junto a cada ajuste e introduzca o seleccione valores:
   - **Configuración del proveedor**:
     - Crea un nuevo bloque, selecciona un bloque existente si ya existe uno en BlueXP o trae tu propio bloque que almacenará los backups.
     - Cuenta, región, clave de acceso y clave secreta de AWS para las credenciales de AWS

       "Si desea traer su propio cubo, consulte Agregar cubos S3".
   - **Cifrado**: Si está creando un nuevo depósito de S3, introduzca la información de clave de cifrado que le haya proporcionado el proveedor. Si eligió un depósito existente, la información de cifrado ya estará disponible.

     De forma predeterminada, los datos del bloque se cifran con claves gestionadas por AWS. Puede seguir utilizando claves administradas por AWS o puede gestionar el cifrado de sus datos utilizando sus propias claves.
   - **Redes**: Elige el espacio IP y si vas a usar un Punto Final Privado.
     - El espacio IP es el clúster donde residen los volúmenes del que se desea incluir en un backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.

- Opcionalmente, seleccione si va a utilizar un punto final privado de AWS (PrivateLink) que haya configurado previamente.

  Si desea utilizar AWS PrivateLink, consulte "AWS PrivateLink para Amazon S3".

- * Bloqueo de respaldo*: Elija si desea que el servicio proteja las copias de seguridad de ser modificadas o eliminadas. Esta opción utiliza la tecnología DataLock de NetApp. Cada copia de seguridad se bloqueará durante el período de retención, o durante un mínimo de 30 días, más un período de búfer de hasta 14 días.

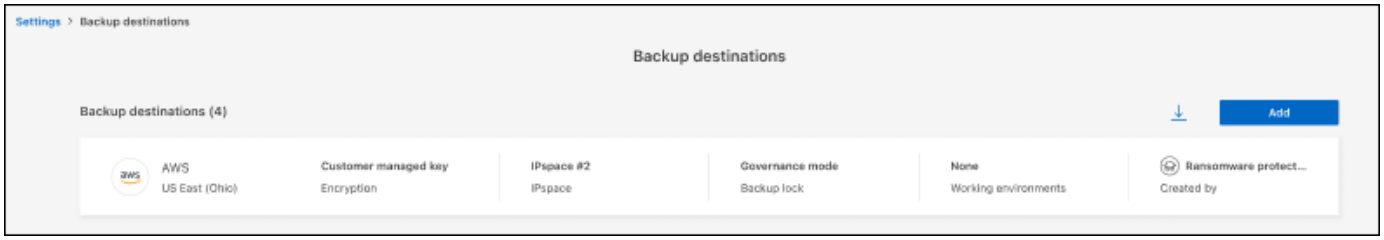
  Si configura ahora el ajuste de bloqueo de copia de seguridad, no es posible cambiarlo más tarde después de configurar el destino de copia de seguridad.

  - **Modo de gobierno**: Los usuarios específicos (con el permiso S3:BypassGovernanceRetention) pueden sobrescribir o eliminar archivos protegidos durante el período de retención.
  - **Modo de cumplimiento**: Los usuarios no pueden sobrescribir ni eliminar los archivos de copia de seguridad protegidos durante el período de retención.

5. Seleccione **Agregar**.

Resultado

El nuevo destino de copia de seguridad se agrega a la lista de destinos de copia de seguridad.



Preguntas frecuentes sobre la protección contra ransomware de BlueXP

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Acceso

¿Cuál es la URL de protección contra ransomware de BlueXP?
Para la URL, en un navegador, introduzca: "https://console.bluexp.netapp.com/" Para acceder a la consola BlueXP.

¿Necesitas una licencia para usar la protección contra ransomware de BlueXP?
No se requiere un archivo de licencia de NetApp (NLF). La versión previa de la protección contra ransomware de BlueXP no requiere ninguna licencia especial. Todas las licencias de vista previa son licencias de evaluación.

Para la versión previa de este servicio, se requiere una licencia de servicio de backup y recuperación de BlueXP.

Para la versión de vista previa, NetApp ayuda a configurar la evaluación y las licencias necesarias.

¿Cómo habilitas la protección contra ransomware de BlueXP?
La protección frente al ransomware de BlueXP no requiere habilitación. La opción de protección frente a ransomware se habilita automáticamente en la navegación de la izquierda de BlueXP.

Para la versión de vista previa, debes registrarte o ponerte en contacto con tu representante de ventas de NetApp para probar este servicio. Una vez que utilices BlueXP Connector, incluirá las prestaciones adecuadas para el servicio.

¿La protección contra ransomware de BlueXP está disponible en modos estándar, restringido y privado?
Por el momento, la protección contra ransomware de BlueXP solo está disponible en modo estándar. Manténgase atento para obtener más información.

Para ver una explicación sobre estos modos en todos los servicios de BlueXP, consulte "Modos de implementación de BlueXP".

- ¿Cómo se manejan los permisos de acceso?**
  Solo los administradores de cuentas tienen la capacidad de iniciar el servicio y detectar cargas de trabajo (porque esto implica comprometerse con el uso de un recurso). Cualquier rol puede realizar interacciones posteriores.
- ¿Qué resolución de dispositivo es la mejor?**
  La resolución de dispositivo recomendada para la protección contra ransomware de BlueXP es 1920x1080 o superior.
- ¿Qué navegador debo usar?**
  Cualquier navegador moderno funcionará.

Interacción con otros servicios

¿La protección contra ransomware de BlueXP es consciente de las configuraciones de protección hechas en NetApp ONTAP?
Sí, la protección frente a ransomware de BlueXP detecta las programaciones de Snapshot establecidas en ONTAP.

Si estableces una política usando la protección contra ransomware de BlueXP, ¿tienes que hacer cambios futuros solo en este servicio?
Te recomendamos que realices cambios de política en el servicio de protección contra ransomware de BlueXP.

Cargas de trabajo

- ¿Qué compone una carga de trabajo?**
  Una carga de trabajo incluye todos los volúmenes que utiliza una única instancia de aplicación. Por ejemplo, una instancia de Oracle DB desplegada en ora3.host.com puede tener vol1 y vol2 para sus datos y registros, respectivamente. Esos volúmenes juntos constituyen la carga de trabajo para esa instancia específica de la instancia de Oracle DB.

¿Cómo prioriza la protección contra ransomware de BlueXP los datos de carga de trabajo?
La prioridad de los datos para la versión Preview viene determinada por las copias snapshot realizadas y las copias de seguridad programadas.

La prioridad de la carga de trabajo se determina en las siguientes frecuencias de Snapshot:

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

Nuevo volumen añadido, pero aún no aparece
Si añadió un volumen nuevo a su entorno, inicie la detección nuevamente y aplique políticas de protección para proteger ese nuevo volumen.

La consola no muestra todas mis cargas de trabajo. ¿Qué podría estar mal?
Actualmente, solo se admiten volúmenes NFS. Los volúmenes iSCSI, los volúmenes CIFS y otras configuraciones no compatibles se filtran y no aparecen en la consola.

Políticas de protección

¿Coexisten las políticas de ransomware de BlueXP con los otros tipos de políticas de cargas de trabajo?
En este momento, el backup y recuperación de datos de BlueXP (Cloud Backup) admite una política de backup por volumen. Por ello, el backup y la recuperación de BlueXP y la protección frente a ransomware de BlueXP comparten las políticas de backup.

Las copias Snapshot no están limitadas y se pueden añadir por separado en cada servicio.