



# **Manos a la obra**

## **Ransomware Protection**

NetApp  
February 20, 2023

# Tabla de Contenido

- Manos a la obra ..... 1
  - Obtenga más información sobre la protección contra ransomware ..... 1
  - Supervisar el estado de las alertas de ransomware ..... 3

# Manos a la obra

## Obtenga más información sobre la protección contra ransomware

Los ataques de ransomware pueden suponer un coste comercial, recursos y reputación. El servicio de protección contra ransomware BlueXP (anteriormente Cloud Manager) le permite ver información relevante sobre ciberseguridad y evaluar la flexibilidad que ofrece su organización a un ataque cibernético. También incluye una lista de alertas y soluciones para proteger los datos.

["Obtenga información sobre los casos de uso de la protección contra Ransomware"](#).



El servicio de protección contra ransomware es actualmente una oferta beta.

### Funciones

La protección de ransomware proporciona un único punto de visibilidad y control para gestionar y refinar la seguridad de datos en diversos entornos de trabajo y capas de infraestructura con el fin de responder mejor a las amenazas a medida que se producen. Actualmente, proporciona varias funciones que le ayudan en sus esfuerzos de protección del ciberalmacenamiento. Las funciones actuales identifican cuándo:

- Los volúmenes de sus entornos de trabajo no se protegen realizando copias Snapshot periódicas.
- Los volúmenes de sus entornos de trabajo no se protegen mediante la creación de backups en el cloud con ["Backup en el cloud"](#).
- Los volúmenes de sus entornos de trabajo están protegidos contra la modificación y eliminación en el almacenamiento WORM mediante la tecnología ONTAP SnapLock. ["Obtenga más información acerca de SnapLock"](#).
- Los datos de sus entornos de trabajo y orígenes de datos no se analizan con ["Cloud Data SENSE"](#) identificar problemas relacionados con el cumplimiento de normativas y la privacidad y buscar oportunidades de optimización.

Esta funcionalidad también es importante desde el punto de vista de la protección de ransomware, gracias a lo cual puede comprender mejor dónde están ubicados sus datos importantes (confidenciales, vitales para el negocio), de manera que pueda asegurarse de centrarse en su esfuerzo relacionado con la protección.

- No se están realizando backups de sus categorías más importantes de datos en caso de que tenga que recuperarse debido a un ataque de ransomware.
- Se ha producido un aumento anómalo del porcentaje de archivos cifrados en un entorno de trabajo o en un origen de datos.

Esto puede ser un indicador de que un ataque de ransomware ha comenzado en su red.

- Los datos confidenciales se encuentran en archivos de un entorno de trabajo o origen de datos y el nivel de permisos de acceso es demasiado alto.
- Se han agregado usuarios a los grupos de administradores de dominio de Active Directory.
- La versión del software ONTAP de los clústeres es antigua y debe actualizarse para proporcionar las

mejores funciones de protección y seguridad, y las más recientes.

- La auditoría del sistema de archivos NAS no está habilitada en los sistemas ONTAP.

Al habilitar la auditoría CIFS, se generan eventos de auditoría para los administradores del sistema que realizan un seguimiento de la información, como los cambios de permisos de carpeta, los intentos fallidos de leer o escribir archivos y cuándo se han creado, modificado o eliminado archivos.

- Las funciones antivirus ransomware integradas no están habilitadas en sus sistemas ONTAP.

Las funciones ONTAP antiransomware detectan de forma proactiva y alertan de una actividad anormal que puede indicar un ataque de ransomware.

- Cuando ONTAP contra el ransomware está habilitado en sus sistemas, el número de incidentes de ransomware aparecerá como alertas.
- El número de vulnerabilidades de alta, media y baja seguridad que la herramienta Active IQ Digital Advisor ha encontrado en sus clústeres de ONTAP.

Puede ver la vulnerabilidad y seguir la acción recomendada para resolver el problema.

["Vea cómo ver estos posibles problemas en el panel de protección contra ransomware."](#)

Cuando se utilizan sistemas Cloud Volumes ONTAP, existen algunas protecciones adicionales de ransomware que se pueden implementar directamente desde el entorno de trabajo. ["Vea cómo añadir protección adicional contra el ransomware"](#).

## Entornos de trabajo y fuentes de datos compatibles

["Cloud Data SENSE"](#) Es un requisito previo para utilizar el servicio de protección contra ransomware. Una vez que se ha instalado y activado Data Sense, puede usar la protección de ransomware para ver cómo se puede resistir la resistencia de sus datos a un ataque cibernético en los siguientes tipos de entornos de trabajo y orígenes de datos:

### Entornos de trabajo:

- Cloud Volumes ONTAP (implementado en AWS, Azure o GCP)
- Clústeres de ONTAP en las instalaciones
- Azure NetApp Files
- Amazon FSX para ONTAP
- Amazon S3

### Fuentes de datos:

- Recursos compartidos de archivos que no son de NetApp
- Almacenamiento de objetos (que utiliza el protocolo S3)
- Bases de datos (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL y SAP HANA, SQL SERVER)
- Cuentas de OneDrive
- Cuentas en línea y en las instalaciones de SharePoint
- Cuentas de Google Drive

Ransomware Protection también supervisa su configuración global de Active Directory, si lo tiene ["Lo configuró"](#)

en Cloud Data Sense".

## Cómo funciona la protección contra Ransomware

En un alto nivel, la protección contra Ransomware funciona de la siguiente manera:


1. La protección de ransomware recopila información de sus sistemas de almacenamiento, Cloud Data Sense, Cloud Backup y otros recursos de BlueXP y NetApp para completar la consola de protección de ransomware.
2. Usted utiliza el panel de protección contra ransomware para obtener una descripción general de la protección de sus sistemas.
3. Utilice las herramientas de generación de informes proporcionadas para ayudarle en sus esfuerzos de protección del almacenamiento cibernético.

## Coste

No hay costo separado para el servicio de protección contra Ransomware durante la beta.

## Supervisar el estado de las alertas de ransomware

Puede ver el estado de las alertas de ransomware en el Centro de notificación de BlueXP. También puede configurar notificaciones para que se envíen por correo electrónico, de modo que se le pueda informar de la actividad importante del sistema incluso si no ha iniciado sesión en el sistema.

El Centro de notificaciones realiza un seguimiento del progreso de los incidentes de ransomware para poder verificar si se han resuelto o no. Puede mostrar las notificaciones haciendo clic en  En la barra de menús de BlueXP. También puede configurar BlueXP para que envíe notificaciones por correo electrónico como alertas.

En este momento, hay un evento que activará las alertas por correo electrónico:

- Posible ataque de ransomware detectado en su sistema

De forma predeterminada, los administradores de cuentas de BlueXP recibirán correos electrónicos para todas las alertas "críticas" y "recomendaciones". Todos los demás usuarios y destinatarios están configurados, de forma predeterminada, para no recibir ningún correo electrónico de notificación. Los correos electrónicos se pueden enviar a todos los usuarios de BlueXP que formen parte de su cuenta de Cloud de NetApp, o a cualquier otro destinatario que necesite conocer sobre incidentes de protección contra ransomware.

Tendrá que seleccionar el tipo de notificación "crítico" para recibir las alertas por correo electrónico de protección contra ransomware.

["Obtenga más información sobre el Centro de notificaciones"](#) y cómo enviar correos electrónicos de alerta para incidentes de protección contra ransomware.

## Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.