Notas de la versión

NetApp Ransomware Resilience

NetApp
February 19, 2026

This PDF was generated from https://docs.netapp.com/es-es/data-services-ransomware-resilience/whats-new.html on February 19, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Notas de la versión

Novedades en NetApp Ransomware Resilience

Descubra las novedades en NetApp Ransomware Resilience.

16 febrero 2026

Soporte de Azure NetApp Files

Ransomware Resilience ahora es compatible con los sistemas Azure NetApp Files, lo que te permite detectar y responder eficazmente a las amenazas de ransomware en Azure NetApp Files. Cuando descubres cargas de trabajo, Ransomware Resilience ahora presenta Azure NetApp Files y las muestra en el panel de protección. El soporte de Ransomware Resilience para Azure NetApp Files incluye estrategias de detección y protección solo con instantáneas. El soporte para Azure NetApp Files está actualmente en vista previa.

Para más información, consulta el enlace: para más información, consulta "Aprenda sobre la resiliencia frente al ransomware".

Excluir usuarios de las alertas de comportamiento del usuario

Ransomware Resilience ahora te permite excluir a usuarios específicos de las alertas de comportamiento del usuario. Excluir a usuarios de confianza puede evitar falsos positivos y alertas innecesarias.

Para más información, consulta el enlace: para más información, consulta "Excluir usuarios de alertas".

Soporte de grupo de protección para la actividad de comportamiento del usuario

Los grupos de protección de Ransomware Resilience ahora admiten políticas de detección para detectar comportamientos sospechosos de los usuarios. Cuando aplicas una estrategia de protección contra ransomware a un grupo de protección, se aplica una política en todas las cargas de trabajo, lo que agiliza la gestión de tu postura de ciberseguridad.

Para más información, consulta "Crear un grupo de protección".

19 de enero de 2026

Volúmenes no compatibles

Los informes de Ransomware Resilience ahora capturan información sobre volúmenes admitidos y no admitidos en el informe **Summary**. Usa esta información para diagnosticar por qué los volúmenes de un sistema podrían no ser elegibles para la protección contra ransomware.

Para obtener más información, consulte "Descargar informes de Ransomware Resilience".

12 de enero de 2026

Replicar instantáneas en ONTAP

Ransomware Resilience ahora admite agregar la replicación de instantáneas a un sitio ONTAP secundario. Con los grupos de protección que usan una política de replicación, puedes replicar en el mismo destino o en destinos diferentes para cada carga de trabajo. Puedes crear una estrategia de protección contra ransomware

que incluya replicación o usar la estrategia predefinida.

Para obtener más información, consulte "Proteja las cargas de trabajo en Ransomware Resilience".

Excluir cargas de trabajo de Ransomware Resilience

Ransomware Resilience ahora permite excluir cargas de trabajo específicas de un sistema de la protección y del panel de Ransomware Resilience. Puede excluir cargas de trabajo después del descubrimiento y volver a incluirlas si desea agregar protección contra ransomware. No se le facturarán las cargas de trabajo excluidas.

Para obtener más información, consulte "Excluir cargas de trabajo".

Marcar alertas como en revisión

Ransomware Resilience ahora le permite marcar alertas como "En revisión". Utilice la etiqueta "En revisión" para mejorar la claridad en todo su equipo al clasificar y gestionar amenazas de ransomware activas.

Para obtener más información, consulte "Administrar alertas en Ransomware Resilience".

08 de diciembre de 2025

El bloqueo de extensiones está habilitado a nivel de carga de trabajo

Cuando habilita el bloqueo de extensiones, ahora se habilita en el nivel de carga de trabajo en lugar de en el nivel de máquina virtual de almacenamiento.

Editar el estado de alerta de comportamiento del usuario

Ransomware Resilience ahora le permite editar el estado de las alertas de comportamiento del usuario. Puede descartar y resolver alertas manualmente.

Para obtener más información, consulte "Administrar alertas en Ransomware Resilience".

Compatibilidad con múltiples agentes de consola

Ransomware Resilience ahora admite el uso de múltiples agentes de consola para administrar los mismos sistemas.

Para obtener más información sobre los agentes de consola, consulte"Crear un agente de consola" .

10 de noviembre de 2025

Esta versión incluye mejoras generales.

6 de octubre de 2025

La BlueXP ransomware protection ahora es NetApp Ransomware Resilience

El servicio de BlueXP ransomware protection ha pasado a llamarse NetApp Ransomware Resilience.

BlueXP ahora es NetApp Console

La NetApp Console proporciona una gestión centralizada de servicios de almacenamiento y datos en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y

una administración simplificada.

Para obtener más detalles sobre lo que ha cambiado, consulte la "Notas de la versión de la NetApp Console" .

Detección de violaciones de datos

Ransomware Resilience incluye un nuevo mecanismo de detección que se puede activar en unos pocos pasos para detectar lecturas anómalas del usuario como un indicador temprano de violación de datos. La resiliencia ante ransomware recopila y analiza eventos de lectura del usuario mediante la creación de una línea de base histórica, que es un perfil del comportamiento normal esperado a partir de datos pasados. Cuando la actividad de un nuevo usuario se desvía significativamente de esta norma establecida (por ejemplo, un aumento inesperado de lectura combinado con patrones de lectura sospechosos), se genera una alerta. Ransomware Resilience incluye un modelo de IA para detectar patrones de lectura sospechosos.

A diferencia de la detección de cifrado por ARP en la capa de almacenamiento, la detección de la anomalía en el comportamiento del usuario se realiza en el servicio Ransomware Resilience SaaS mediante la recopilación de eventos FPolicy.

> Debes utilizar el nuevo"Administrador del comportamiento del usuario de Ransomware Resilience y visor del comportamiento del usuario de Ransomware Resilience" Roles para acceder a configuraciones de detección de comportamiento sospechoso de usuarios.

Para obtener más información, consulte"Habilitar la detección de actividad sospechosa de usuarios" y"Ver comportamiento anómalo del usuario" .

Detecciones adicionales de actividad sospechosa del usuario

Además de la detección de violaciones de datos, Ransomware Resilience también detecta los siguientes tipos de alertas según la actividad sospechosa del usuario observada:

- **Destrucción de datos - ataque potencial** - Se crea una alerta con la gravedad del ataque potencial cuando la cantidad de eliminaciones de archivos excede la norma histórica.
- **Comportamiento sospechoso del usuario - posible ataque**: se crea una alerta con la gravedad del posible ataque cuando se observan operaciones de lectura, cambio de nombre y eliminación en una secuencia similar a un ataque de ransomware.
- **Comportamiento sospechoso del usuario - Advertencia** - Se crea una alerta con la gravedad de advertencia cuando el número total de actividades de archivo (lectura, eliminación, cambio de nombre, etc.) excede la norma histórica.

Nuevos roles de usuario para la detección de violaciones de datos

Para administrar las alertas de actividad sospechosa de los usuarios, Ransomware Resilience ha introducido dos nuevos roles para que los administradores de la organización de la consola otorguen acceso a la detección de actividad sospechosa de los usuarios: administrador de comportamiento de usuarios de Ransomware Resilience y visor de comportamiento de usuarios de Ransomware Resilience.

Debe ser un administrador de comportamiento de usuario para configurar las opciones de comportamiento de usuario sospechoso. El rol de administrador de Ransomware Resilience no es compatible con la configuración de ajustes de comportamiento de usuarios sospechosos.

Para obtener más información, consulte "Acceso basado en roles de NetApp Ransomware Resilience" .

12 de agosto de 2025

Esta versión incluye mejoras generales.

15 de julio de 2025

Soporte de carga de trabajo SAN

Esta versión incluye soporte para cargas de trabajo SAN en la BlueXP ransomware protection. Ahora puede proteger cargas de trabajo SAN además de cargas de trabajo NFS y CIFS.

Para obtener más información, consulte "Requisitos previos para la BlueXP ransomware protection" .

Protección mejorada de la carga de trabajo

Esta versión mejora el proceso de configuración para cargas de trabajo con políticas de instantáneas y respaldo de otras herramientas de NetApp , como SnapCenter o BlueXP backup and recovery. En versiones anteriores, la BlueXP ransomware protection descubría las políticas de otras herramientas y solo le permitía cambiar la política de detección. Con esta versión, ahora puede reemplazar las políticas de instantáneas y copias de seguridad con las políticas de BlueXP ransomware protection o continuar usando las políticas de otras herramientas.

Para más detalles, consulte"Proteger las cargas de trabajo" .

Notificaciones por correo electrónico

Si la BlueXP ransomware protection detecta un posible ataque, aparece una notificación en Notificaciones de BlueXP y se envía un correo electrónico a la dirección de correo electrónico que usted configuró.

El correo electrónico incluye información sobre la gravedad, la carga de trabajo afectada y un enlace a la alerta en la pestaña **Alertas** de BlueXP ransomware protection .

Si configuró un sistema de gestión de eventos y seguridad (SIEM) en la BlueXP ransomware protection, el servicio envía detalles de alerta a su sistema SIEM.

Para más detalles, consulte"Gestionar alertas de ransomware detectadas" .

9 de junio de 2025

Actualizaciones de la página de destino

Esta versión incluye actualizaciones a la página de inicio de BlueXP ransomware protection que facilitan el inicio de la prueba gratuita y el descubrimiento.

Actualizaciones de simulacros de preparación

Anteriormente, se podía ejecutar un simulacro de preparación ante ransomware simulando un ataque en una nueva carga de trabajo de muestra. Con esta función, puede investigar el ataque simulado y recuperar la carga de trabajo. Utilice esta función para probar las notificaciones de alerta, la respuesta y la recuperación. Ejecute y programe estos simulacros con tanta frecuencia como sea necesario.

Con esta versión, puede usar un nuevo botón en el Panel de BlueXP ransomware protection para ejecutar un simulacro de preparación para ransomware en una carga de trabajo de prueba, lo que le facilita simular ataques de ransomware, investigar su impacto y recuperar cargas de trabajo de manera eficiente, todo dentro

de un entorno controlado.

Ahora puede ejecutar simulacros de preparación en cargas de trabajo CIFS (SMB) además de en cargas de trabajo NFS.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Habilitar actualizaciones de BlueXP classification

Antes de utilizar la BlueXP classification dentro del servicio de BlueXP ransomware protection , debe habilitar la BlueXP classification para escanear sus datos. La clasificación de datos le ayuda a encontrar información de identificación personal (PII), lo que puede aumentar los riesgos de seguridad.

Puede implementar la BlueXP classification en una carga de trabajo de uso compartido de archivos desde la BlueXP ransomware protection. En la columna **Exposición de privacidad**, seleccione la opción **Identificar exposición**. Si ha habilitado el servicio de clasificación, esta acción identifica la exposición. De lo contrario, con esta versión, un cuadro de diálogo presenta la opción de implementar la BlueXP classification. Seleccione **Implementar** para ir a la página de inicio del servicio de BlueXP classification , donde puede implementar ese servicio. O

Para más detalles, consulta "Implementar la BlueXP classification en la nube" y para usar el servicio dentro de BlueXP ransomware protection, consulta "Escanee en busca de información de identificación personal con la BlueXP classification".

13 de mayo de 2025

Informes de entornos de trabajo no compatibles con la BlueXP ransomware protection

Durante el flujo de trabajo de descubrimiento, la BlueXP ransomware protection informa más detalles cuando pasa el cursor sobre Cargas de trabajo compatibles o No compatibles. Esto le ayudará a comprender por qué el servicio de BlueXP ransomware protection no detecta algunas de sus cargas de trabajo.

Hay muchas razones por las cuales el servicio no admite un entorno de trabajo, por ejemplo, la versión de ONTAP en su entorno de trabajo podría ser inferior a la versión requerida. Cuando pasa el cursor sobre un entorno de trabajo no compatible, aparece una información sobre herramientas que muestra el motivo.

Puede ver los entornos de trabajo no compatibles durante el descubrimiento inicial, donde también puede descargar los resultados. También puede ver los resultados del descubrimiento desde la opción **Descubrimiento de carga de trabajo** en la página Configuración.

Para más detalles, consulte "Descubra las cargas de trabajo en la BlueXP ransomware protection" .

29 de abril de 2025

Compatibilidad con Amazon FSx for NetApp ONTAP

Esta versión es compatible con Amazon FSx for NetApp ONTAP. Esta función le ayuda a proteger sus cargas de trabajo de FSx para ONTAP con la BlueXP ransomware protection.

FSx for ONTAP es un servicio totalmente administrado que proporciona la potencia del almacenamiento NetApp ONTAP en la nube. Proporciona las mismas características, rendimiento y capacidades administrativas que utiliza en sus instalaciones con la agilidad y escalabilidad de un servicio nativo de AWS.

Se realizaron los siguientes cambios en el flujo de trabajo de BlueXP ransomware protection :

- Discovery incluye cargas de trabajo en FSx para entornos de trabajo de ONTAP 9.15.
- La pestaña Protección muestra las cargas de trabajo en FSx para entornos ONTAP . En este entorno, debe realizar operaciones de respaldo utilizando el servicio de respaldo FSx para ONTAP . Puede restaurar estas cargas de trabajo utilizando instantáneas de BlueXP ransomware protection .

> Las políticas de respaldo para una carga de trabajo que se ejecuta en FSx para ONTAP no se pueden configurar en BlueXP. Cualquier política de respaldo existente establecida en Amazon FSx for NetApp ONTAP permanecerá sin cambios.

- Los incidentes de alerta muestran el nuevo entorno de trabajo de FSx para ONTAP .

Para más detalles, consulte "Obtenga más información sobre la BlueXP ransomware protection y los entornos de trabajo" .

Para obtener información sobre las opciones admitidas, consulte la "Limitaciones de la BlueXP ransomware protection" .

Se necesita el rol de acceso a BlueXP

Ahora necesita uno de los siguientes roles de acceso para ver, descubrir o administrar la BlueXP ransomware protection: administrador de la organización, administrador de carpeta o proyecto, administrador de protección contra ransomware o visor de protección contra ransomware.

"Obtenga información sobre los roles de acceso de BlueXP para todos los servicios" .

14 de abril de 2025

Informes de simulacros de preparación

Con esta versión, puedes revisar los informes de simulacros de preparación para ataques de ransomware. Un simulacro de preparación le permite simular un ataque de ransomware en una carga de trabajo de muestra recién creada. Luego, investigue el ataque simulado y recupere la carga de trabajo de muestra. Esta función le ayuda a saber que está preparado en caso de un ataque de ransomware real al probar los procesos de notificación de alerta, respuesta y recuperación.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Nuevos roles y permisos de control de acceso basados en roles

Anteriormente, podía asignar roles y permisos a los usuarios en función de sus responsabilidades, lo que le ayudaba a administrar el acceso de los usuarios a la BlueXP ransomware protection. Con esta versión, hay dos nuevos roles específicos para la BlueXP ransomware protection con permisos actualizados. Los nuevos roles son:

- Administrador de protección contra ransomware
- Visor de protección contra ransomware

Para obtener detalles sobre los permisos, consulte "Acceso basado en roles a las funciones de BlueXP ransomware protection" .

Mejoras en los pagos

Esta versión incluye varias mejoras en el proceso de pago.

Para más detalles, consulte "Configurar opciones de licencia y pago" .

10 de marzo de 2025

Simular un ataque y responder

Con esta versión, simule un ataque de ransomware para probar su respuesta a una alerta de ransomware. Esta función le ayuda a saber que está preparado en caso de un ataque de ransomware real al probar los procesos de notificación de alerta, respuesta y recuperación.

Para más detalles, consulte "Realizar un simulacro de preparación para un ataque de ransomware" .

Mejoras en el proceso de descubrimiento

Esta versión incluye mejoras en los procesos de descubrimiento y redescubrimiento selectivo:

- Con esta versión, puede descubrir cargas de trabajo recién creadas que se agregaron a los entornos de trabajo seleccionados previamente.
- También puedes seleccionar *nuevos* entornos de trabajo en esta versión. Esta función le ayuda a proteger las nuevas cargas de trabajo que se agregan a su entorno.
- Puede realizar estos procesos de descubrimiento durante el proceso de descubrimiento inicialmente o dentro de la opción Configuración.

Para más detalles, consulte "Descubra cargas de trabajo recién creadas para entornos de trabajo previamente seleccionados" y "Configurar funciones con la opción Configuración" .

Alertas generadas cuando se detecta un cifrado alto

Con esta versión, puede ver alertas cuando se detecta un cifrado alto en sus cargas de trabajo incluso sin grandes cambios en la extensión de archivo. Esta función, que utiliza la inteligencia artificial de ONTAP Autonomous Ransomware Protection (ARP), lo ayuda a identificar cargas de trabajo que corren riesgo de sufrir ataques de ransomware. Utilice esta función y descargue la lista completa de archivos afectados con o sin cambios de extensión.

Para más detalles, consulte "Responder a una alerta de ransomware detectada" .

16 de diciembre de 2024

Detecte comportamientos anómalos de los usuarios mediante Data Infrastructure Insights Storage Workload Security

Con esta versión, puede utilizar Data Infrastructure Insights Storage Workload Security para detectar comportamientos anómalos de los usuarios en sus cargas de trabajo de almacenamiento. Esta función le ayuda a identificar posibles amenazas a la seguridad y a bloquear usuarios potencialmente maliciosos para proteger sus datos.

Para más detalles, consulte "Responder a una alerta de ransomware detectada" .

Antes de usar Data Infrastructure Insights Storage Workload Security para detectar un comportamiento anómalo del usuario, debe configurar la opción mediante la opción **Configuración** de BlueXP ransomware protection .

Referirse a "Configurar los ajustes de BlueXP ransomware protection" .

Seleccione cargas de trabajo para descubrir y proteger

Con esta versión, ahora puedes hacer lo siguiente:

- Dentro de cada Conector, seleccione los entornos de trabajo donde desea descubrir cargas de trabajo. Esta función puede resultarle beneficiosa si desea proteger cargas de trabajo específicas en su entorno y no otras.
- Durante el descubrimiento de carga de trabajo, puede habilitar el descubrimiento automático de cargas de trabajo por conector. Esta función le permite seleccionar las cargas de trabajo que desea proteger.
- Descubra cargas de trabajo recién creadas para entornos de trabajo previamente seleccionados.

Referirse a "Descubra las cargas de trabajo" .

7 de noviembre de 2024

Habilitar la clasificación de datos y el escaneo de información de identificación personal (PII)

Con esta versión, puede habilitar la BlueXP classification, un componente central de la familia BlueXP , para escanear y clasificar datos en sus cargas de trabajo de uso compartido de archivos. La clasificación de datos le ayuda a identificar si sus datos incluyen información personal o privada, lo que puede aumentar los riesgos de seguridad. Este proceso también afecta la importancia de la carga de trabajo y le ayuda a garantizar que está protegiendo las cargas de trabajo con el nivel de protección adecuado.

El escaneo de datos PII en la BlueXP ransomware protection generalmente está disponible para los clientes que implementaron la BlueXP classification. La BlueXP classification está disponible como parte de la plataforma BlueXP sin costo adicional y puede implementarse localmente o en la nube del cliente.

Para iniciar el escaneo, en la página Protección, selecciona **Identificar exposición** en la columna Exposición de privacidad del panel Protección. Para más información, consulta "busca datos sensibles de identificación personal con BlueXP classification".

Integración de SIEM con Microsoft Sentinel

Ahora puede enviar datos a su sistema de gestión de eventos y seguridad (SIEM) para el análisis y detección de amenazas mediante Microsoft Sentinel. Anteriormente, podía seleccionar AWS Security Hub o Splunk Cloud como su SIEM.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection".

Prueba gratuita ahora 30 días

Con este lanzamiento, las nuevas implementaciones de BlueXP ransomware protection ahora tienen 30 días de prueba gratuita. Anteriormente, la BlueXP ransomware protection ofrecía una prueba gratuita de 90 días. Si ya está en la prueba gratuita de 90 días, esa oferta continúa durante los 90 días.

Restaurar la carga de trabajo de la aplicación a nivel de archivo para Podman

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede ver una lista de archivos que podrían haber sido afectados por un ataque e identificar aquellos que desea restaurar. Anteriormente, si los conectores BlueXP de una organización (anteriormente una cuenta) usaban Podman, esta función estaba deshabilitada. Ahora está habilitado para Podman. Puede dejar que la BlueXP ransomware protection elija los archivos a restaurar, puede cargar un archivo CSV que enumere todos los archivos afectados por una alerta o puede identificar manualmente qué archivos desea restaurar.

"Obtenga más información sobre cómo recuperarse de un ataque de ransomware" .

30 de septiembre de 2024

Agrupación personalizada de cargas de trabajo de recursos compartidos de archivos

Con esta versión, ahora puede agrupar recursos compartidos de archivos en grupos para facilitar la protección de su patrimonio de datos. El servicio puede proteger todos los volúmenes de un grupo al mismo tiempo. Anteriormente, era necesario proteger cada volumen por separado.

"Obtenga más información sobre la agrupación de cargas de trabajo de recursos compartidos de archivos en las estrategias de protección contra ransomware." .

2 de septiembre de 2024

Evaluación de riesgos de seguridad de Digital Advisor

La protección contra ransomware de BlueXP ahora recopila información sobre riesgos de seguridad altos y críticos relacionados con un clúster desde NetApp Digital Advisor. Si se encuentra algún riesgo, la protección contra ransomware de BlueXP te da una recomendación en el panel **Recommended actions**: "Soluciona una vulnerabilidad de seguridad conocida en el clúster <name>." Desde la recomendación en el panel de control, si seleccionas **Review and fix**, se sugiere revisar Digital Advisor y un artículo de Common Vulnerability & Exposure (CVE) para resolver el riesgo de seguridad. Si hay varios riesgos de seguridad, revisa la información en Digital Advisor.

Referirse a "Documentación de Digital Advisor" .

Realizar copias de seguridad en Google Cloud Platform

Con esta versión, puedes establecer un destino de respaldo en un depósito de Google Cloud Platform. Anteriormente, solo podía agregar destinos de respaldo a NetApp StorageGRID, Amazon Web Services y Microsoft Azure.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection" .

Compatibilidad con Google Cloud Platform

El servicio ahora es compatible con Cloud Volumes ONTAP para Google Cloud Platform para la protección del almacenamiento. Anteriormente, el servicio solo admitía Cloud Volumes ONTAP para Amazon Web Services y Microsoft Azure junto con NAS local.

"Obtenga información sobre la BlueXP ransomware protection y las fuentes de datos compatibles, los destinos de copia de seguridad y los entornos de trabajo." .

Control de acceso basado en roles

Ahora puede limitar el acceso a actividades específicas con el control de acceso basado en roles (RBAC). La BlueXP ransomware protection utiliza dos roles de BlueXP: administrador de cuenta de BlueXP y administrador sin cuenta (visor).

Para obtener detalles sobre las acciones que puede realizar cada rol, consulte "Privilegios de control de acceso basados en roles" .

5 de agosto de 2024

Detección de amenazas con Splunk Cloud

Puede enviar datos automáticamente a su sistema de gestión de eventos y seguridad (SIEM) para analizar y detectar amenazas. Con versiones anteriores, solo podía seleccionar AWS Security Hub como su SIEM. Con esta versión, puede seleccionar AWS Security Hub o Splunk Cloud como su SIEM.

"Obtenga más información sobre cómo configurar los ajustes de BlueXP ransomware protection" .

1 de julio de 2024

Traiga su propia licencia (BYOL)

Con esta versión, puede utilizar una licencia BYOL, que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp .

"Obtenga más información sobre la configuración de licencias" .

Restaurar la carga de trabajo de la aplicación a nivel de archivo

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede ver una lista de archivos que podrían haber sido afectados por un ataque e identificar aquellos que desea restaurar. Puede dejar que la BlueXP ransomware protection elija los archivos a restaurar, puede cargar un archivo CSV que enumere todos los archivos afectados por una alerta o puede identificar manualmente qué archivos desea restaurar.

Con esta versión, si todos los conectores BlueXP de una cuenta no usan Podman, se habilita la función de restauración de un solo archivo. De lo contrario, se deshabilitará para esa cuenta.

"Obtenga más información sobre cómo recuperarse de un ataque de ransomware" .

Descargar una lista de archivos afectados

Antes de restaurar una carga de trabajo de la aplicación a nivel de archivo, ahora puede acceder a la página Alertas para descargar una lista de archivos afectados en un archivo CSV y luego usar la página Recuperación para cargar el archivo CSV.

"Obtenga más información sobre cómo descargar archivos afectados antes de restaurar una aplicación" .

Eliminar plan de protección

Con esta versión, ahora puedes eliminar una estrategia de protección contra ransomware.

"Obtenga más información sobre la protección de las cargas de trabajo y la gestión de estrategias de protección contra ransomware." .

10 de junio de 2024

Bloqueo de copia de instantáneas en el almacenamiento principal

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.

"Obtenga más información sobre cómo proteger las cargas de trabajo y habilitar el bloqueo de copias de seguridad en una estrategia de protección contra ransomware." .

Compatibilidad con Cloud Volumes ONTAP para Microsoft Azure

Esta versión es compatible con Cloud Volumes ONTAP para Microsoft Azure como sistema además de Cloud Volumes ONTAP para AWS y ONTAP NAS local.

"Inicio rápido de Cloud Volumes ONTAP en Azure"

"Obtenga más información sobre la BlueXP ransomware protection" .

Microsoft Azure agregado como destino de respaldo

Ahora puede agregar Microsoft Azure como destino de respaldo junto con AWS y NetApp StorageGRID.

"Obtenga más información sobre cómo configurar los ajustes de protección" .

14 de mayo de 2024

Actualizaciones de licencias

Puedes registrarte para una prueba gratuita de 90 días. Pronto podrás comprar una suscripción de pago por uso con Amazon Web Services Marketplace o traer tu propia licencia de NetApp .

"Obtenga más información sobre la configuración de licencias" .

Protocolo CIFS

El servicio ahora admite ONTAP local y Cloud Volumes ONTAP en sistemas AWS mediante protocolos NFS y CIFS. La versión anterior solo admitía el protocolo NFS.

Detalles de la carga de trabajo

Esta versión ahora proporciona más detalles en la información de la carga de trabajo de Protección y otras páginas para una mejor evaluación de la protección de la carga de trabajo. Desde los detalles de la carga de trabajo, puede revisar la política asignada actualmente y revisar los destinos de respaldo configurados.

"Obtenga más información sobre cómo ver los detalles de la carga de trabajo en las páginas de Protección" .

Protección y recuperación consistentes con las aplicaciones y las máquinas virtuales

Ahora puede realizar una protección consistente con las aplicaciones con el software NetApp SnapCenter y una protección consistente con las máquinas virtuales con el SnapCenter Plug-in for VMware vSphere, logrando un estado inactivo y consistente para evitar una posible pérdida de datos más adelante si se necesita recuperación. Si se requiere recuperación, puede restaurar la aplicación o la máquina virtual a cualquiera de los estados disponibles anteriormente.

"Obtenga más información sobre la protección de las cargas de trabajo" .

Estrategias de protección contra ransomware

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 este servicio:

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

"Obtenga más información sobre la protección de las cargas de trabajo" .

Detección de amenazas

Ahora es posible habilitar la detección de amenazas mediante un sistema de gestión de eventos y seguridad (SIEM) de terceros. El Panel de Control ahora muestra una nueva recomendación para "Habilitar detección de amenazas", que se puede configurar en la página de Configuración.

"Obtenga más información sobre cómo configurar las opciones de Configuración" .

Descartar alertas de falsos positivos

Desde la pestaña Alertas, ahora puede descartar falsos positivos o decidir recuperar sus datos de inmediato.

"Obtenga más información sobre cómo responder a una alerta de ransomware" .

Estado de detección

Aparecen nuevos estados de detección en la página Protección que muestran el estado de la detección de ransomware aplicada a la carga de trabajo.

"Obtenga más información sobre cómo proteger cargas de trabajo y visualizar estados de protección" .

Descargar archivos CSV

Puede descargar archivos CSV* desde las páginas Protección, Alertas y Recuperación.

"Obtenga más información sobre cómo descargar archivos CSV desde el Panel de control y otras páginas" .

Enlace de documentación

El enlace Ver documentación ahora está incluido en la interfaz de usuario. Puede acceder a esta documentación desde el Panel de control vertical **Acciones***  **opción. Seleccione *Novedades** para ver los detalles en las Notas de la versión o **Documentación** para ver la página de inicio de la documentación de BlueXP ransomware protection .

BlueXP backup and recovery

Ya no es necesario que el servicio de BlueXP backup and recovery esté habilitado en el sistema. Ver "prerrequisitos" . El servicio de BlueXP ransomware protection ayuda a configurar un destino de copia de seguridad a través de la opción Configuración. Ver "Configurar ajustes" .

Opción de configuración

Ahora puede configurar destinos de respaldo en la configuración de BlueXP ransomware protection .

"Obtenga más información sobre cómo configurar las opciones de Configuración" .

5 de marzo de 2024

Gestión de políticas de protección

Además de utilizar políticas predefinidas, ahora puedes crear políticas. "Obtenga más información sobre la gestión de políticas" .

Inmutabilidad en el almacenamiento secundario (DataLock)

Ahora puede hacer que la copia de seguridad sea inmutable en el almacenamiento secundario utilizando la tecnología NetApp DataLock en el almacén de objetos. "Obtenga más información sobre la creación de políticas de protección" .

Copia de seguridad automática en NetApp StorageGRID

Además de usar AWS, ahora puedes elegir StorageGRID como tu destino de respaldo. "Obtenga más información sobre cómo configurar destinos de respaldo" .

Funciones adicionales para investigar posibles ataques

Ahora puede ver más detalles forenses para investigar el posible ataque detectado. "Obtenga más información sobre cómo responder a una alerta de ransomware detectada" .

Proceso de recuperación

Se mejoró el proceso de recuperación. Ahora, puede recuperar volumen por volumen o todos los volúmenes para una carga de trabajo. "Obtenga más información sobre cómo recuperarse de un ataque de ransomware (después de que se hayan neutralizado los incidentes)" .

"Obtenga más información sobre la BlueXP ransomware protection" .

6 de octubre de 2023

El servicio de BlueXP ransomware protection es una solución SaaS para proteger datos, detectar posibles ataques y recuperar datos de un ataque de ransomware.

Para la versión preliminar, el servicio protege cargas de trabajo basadas en aplicaciones de Oracle, almacenes de datos de VM y recursos compartidos de archivos en almacenamiento NAS local, así como Cloud Volumes ONTAP en AWS (usando el protocolo NFS) en organizaciones BlueXP de forma individual y realiza copias de seguridad de los datos en el almacenamiento en la nube de Amazon Web Services.

El servicio de BlueXP ransomware protection proporciona el uso completo de varias tecnologías de NetApp para que su administrador de seguridad de datos o ingeniero de operaciones de seguridad pueda lograr los siguientes objetivos:

- Vea la protección contra ransomware en todas sus cargas de trabajo de un vistazo.
- Obtenga información sobre las recomendaciones de protección contra ransomware

- Mejore la postura de protección según las recomendaciones de BlueXP ransomware protection .
- Asigne políticas de protección contra ransomware para proteger sus principales cargas de trabajo y datos de alto riesgo contra ataques de ransomware.
- Supervise la salud de sus cargas de trabajo contra ataques de ransomware en busca de anomalías en los datos.
- Evalúe rápidamente el impacto de los incidentes de ransomware en su carga de trabajo.
- Recupérese de incidentes de ransomware de forma inteligente restaurando datos y garantizando que no se produzca una reinfección a partir de los datos almacenados.

"Obtenga más información sobre la BlueXP ransomware protection" .

Limitaciones conocidas de NetApp Ransomware Resilience

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o que no interoperan correctamente con él. Revise estas limitaciones cuidadosamente.

Problema con la opción de reinicio del ejercicio de preparación

Si selecciona un volumen ONTAP 9.11.1 para el simulacro de preparación para ataques de ransomware, Ransomware Resilience envía una alerta. Si recupera los datos utilizando la opción "clonar a volumen" y reinicia el taladro, la operación de reinicio falla.

Limitaciones de Amazon FSx for NetApp ONTAP

El sistema Amazon FSx for NetApp ONTAP es compatible con Ransomware Resilience. Las siguientes limitaciones se aplican a Amazon FSx para ONTAP:

- Las políticas de backup no son compatibles con Amazon FSx for ONTAP. En este entorno, deberías realizar las operaciones de backup usando Amazon FSx for backups. Puedes restaurar estas cargas de trabajo usando Ransomware Resilience.
- Las operaciones de restauración se realizan únicamente desde instantáneas.

Limitaciones de Azure NetApp Files

Azure NetApp Files es compatible con Ransomware Resilience. Las siguientes limitaciones aplican a Azure NetApp Files:

- Las estrategias de protección contra ransomware con políticas de backup no son compatibles con Azure NetApp Files. En su lugar, puedes usar el backup de Azure NetApp Files.
- Las estrategias de protección contra ransomware con replicación no son compatibles para Azure NetApp Files.
- Al seleccionar una estrategia de protección, asegúrate de que su planificación de instantáneas sea compatible con Azure NetApp Files. La planificación de instantáneas más frecuente disponible en Azure NetApp Files es horaria.

Información de copyright

Copyright © 2026 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.