Synology®

Proteja su organización contra el ransomware

Se prevé que los ataques de ransomware costarán a las organizaciones un total de un billón de dólares estadounidenses solo en 2023.[1] Los planes de protección de datos con opciones de restauración rápida son cruciales para mitigar el impacto del ransomware y otras formas de ciberdelincuencia.

Date 13 de oct. de 2023

Copias de seguridad: la última línea de defensa cuando ocurre un desastre

Cuando se pierden datos después de una eliminación o modificación maliciosa, las copias de seguridad le permiten restaurar datos críticos y evitar costosos tiempos de inactividad. Aproveche las soluciones de protección de datos de Synology para diseñar una estrategia de copia de seguridad para toda su infraestructura de TI.

Protección completa

Proteja los extremos y las copias de seguridad principales para crear varias redes de seguridad para sus datos.

Recuperación rápida

Reduzca el tiempo de inactividad al mínimo cuando se produce un desastre con opciones de recuperación instantánea.

Almacenamiento inmutable

Evite cambios no autorizados en los datos y las instantáneas.

Copias de seguridad sin licencias

Realice copias de seguridad de todos los datos que su almacenamiento permita, sin limitaciones ni tarifas ocultas.

Protección centralizada contra ransomware

Combine las copias de seguridad de flotas de estaciones de trabajo, servidores, máquinas virtuales y aplicaciones en la nube. Optimice el consumo de almacenamiento y evite los cuellos de botella de ancho de banda con la desduplicación de datos y las tecnologías de copia de seguridad incremental. https://www.synology.com/dsm/solution/infrastructure

Cargas de trabajo físicas

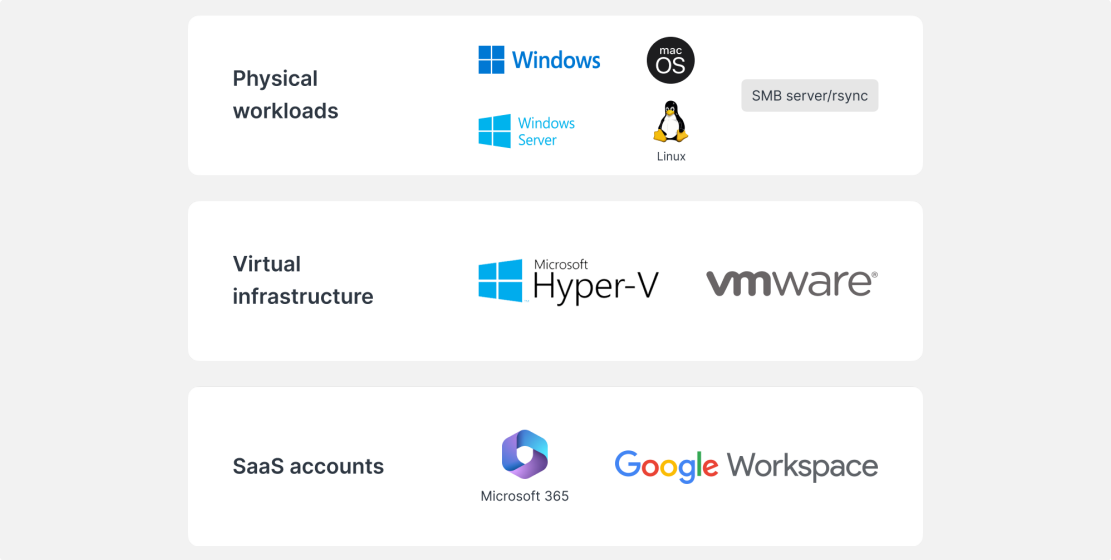
Proteja los extremos de ataques maliciosos con copias de seguridad completas y recuperación flexible a nivel de archivos.

Infraestructura virtual

Realice una copia de seguridad de las máquinas virtuales VMware® vSphere™, Microsoft® Hyper-V® y los LUN con potentes tecnologías de reducción de datos.

Cuentas SaaS

Active la protección continua de los datos almacenados en la nube, con detección automática de cuentas recién agregadas.



Recuperación eficiente

Minimice el tiempo de inactividad de los sistemas de producción críticos mediante la restauración rápida de las copias de seguridad de un sistema Synology local o fuera del sitio.

RTO prácticamente nulo

Monte las imágenes de copia de seguridad en VMware®, Hyper-V® o en Synology Virtual Machine Manager para reanudar el trabajo lo más rápido posible. Restaure las VM a un hipervisor alternativo para evitar interrupciones en el servicio.

RPO mínima

Configure la frecuencia de las copias de seguridad según sus necesidades, minimizando la cantidad de datos que podrían verse afectados durante un ataque. Proteja los sistemas rápidamente gracias a las copias de seguridad incrementales y a la tecnología de desduplicación.

Funcionamiento intuitivo

Permita que los empleados exploren y obtengan una vista previa de correos electrónicos, contactos y archivos desde un cómodo portal antes de restaurarlos, lo que ofrece una experiencia más fácil de usar y reduce la carga para los equipos de TI.

Una capa de protección adicional

Siga la estrategia de copia de seguridad 3-2-1 almacenando un tercer conjunto de datos fuera del sitio o en la nube, protegiendo sus datos contra incendios, desastres naturales o robos.

En servidores fuera del sitio

Almacene copias de seguridad en un servidor de Synology en una ubicación secundaria para defenderse de desastres físicos y replique instantáneas inmutables para mayor protección contra el ransomware.

En la nube

Realice copias de seguridad en cualquier proveedor de almacenamiento en la nube principal, manteniendo sus datos seguros contra el acceso no autorizado a través del cifrado AES-256 del lado del cliente. https://c2.synology.com/storage/nas

De confianza en diferentes industrias

'Synology [...] nos ha permitido reducir el gasto en hardware de servidor [...] al mismo tiempo que nos ha facilitado enormemente las copias de seguridad de la infraestructura y las estaciones de trabajo, el registro del sistema y la administración de archivos'.
https://www.synology.com/company/case_study/Investortools

'Gracias a Active Backup for Business, todas nuestras copias de seguridad están centralizadas y disponibles de forma ininterrumpida, lo que nos ayuda a minimizar el tiempo de inactividad y a cumplir con las regulaciones de la FERPA'.
https://www.synology.com/company/case_study/University_of_Washington

'[...] Active Backup for Business no solo proporciona una velocidad de copia de seguridad impresionante, sino que también hace maravillas a la hora de eliminar los datos duplicados: solo necesitó 28 TB del total de 58 TB que hay en el servidor. [...]'
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

'[...] Active Backup for Business [...] nos permite centralizar y administrar todas las tareas de copia de seguridad desde una única consola. La recuperación rápida y fiable también garantiza la continuidad empresarial'.
https://www.synology.com/company/case_study/UNESCO

Preguntas más frecuentes (P+F)

¿Qué es el ransomware?

El ransomware es un tipo de malware que cifra los archivos de las víctimas. Luego, los atacantes exigen un rescate para restaurar el acceso a los datos, a menudo amenazando con destruir permanentemente los datos si no se paga un rescate. Los ataques de ransomware pueden ser muy perjudiciales y causar pérdidas financieras significativas para individuos y organizaciones. Es importante protegerse uno mismo y los dispositivos contra el ransomware, por ejemplo, manteniendo el software actualizado y realizando copias de seguridad regulares de los archivos.

¿Qué tipos de ransomware existen?

Existen muchos tipos diferentes de ransomware y constantemente se desarrollan nuevas versiones. Algunos de los tipos más comunes de ransomware son:

- **Ransomware de cifrado**: el tipo más común de ransomware cifra los archivos de la víctima para que no pueda acceder a ellos sin la clave de descifrado. Luego, los atacantes exigen el pago de un rescate a cambio de la clave
- **Ransomware bloqueador**: un tipo de ransomware que bloquea a las víctimas para que no puedan acceder a su ordenador cambiando las credenciales de inicio de sesión o mostrando un mensaje que evita que la víctima acceda a su sistema. Luego, los atacantes exigen el pago de un rescate para desbloquear el ordenador
- **Ransomware como servicio (RaaS)**: un modelo empresarial según el cual los atacantes ofrecen ransomware a otros individuos o grupos que quieran llevar a cabo ataques. El primero suele proporcionar el ransomware y manejar los pagos, mientras que el segundo recibe un porcentaje del rescate
- **Scareware**: ransomware diseñado para asustar a las víctimas para que paguen el rescate. Por lo general, implica mostrar advertencias o mensajes de seguridad falsos que afirman que el ordenador de la víctima está infectada con un virus. El atacante entonces exige el pago de un rescate para eliminar la supuesta infección.

¿Cómo se propaga el ransomware?

El ransomware generalmente se propaga a través de correos electrónicos de phishing o mediante el aprovechamiento de vulnerabilidades en un sistema informático. En un ataque de phishing, un atacante enviará un correo electrónico que parece provenir de una fuente legítima, como un banco o una empresa conocida. Con frecuencia, el correo electrónico contiene un enlace o un archivo adjunto que, al hacer clic en él, instalará el ransomware en el ordenador de la víctima. El aprovechamiento de vulnerabilidades en un sistema es similar, excepto que el atacante utilizará un fallo en la seguridad del sistema para instalar el ransomware sin el conocimiento de la víctima. En cualquier caso, una vez instalado el ransomware, puede propagarse rápidamente a otros ordenadores de la misma red.

¿Cuál es el proceso típico de un ataque de ransomware?

El proceso de un ataque de ransomware suele seguir estos pasos:

1. El atacante obtiene acceso al ordenador de una víctima, ya sea mediante el envío de un correo electrónico de phishing o mediante el aprovechamiento de una vulnerabilidad en el sistema.
2. Una vez que el atacante tiene acceso al ordenador de la víctima, instalará el ransomware en el sistema.
3. A continuación, el ransomware cifrará los archivos de la víctima y el usuario no podrá acceder a ellos.
4. El atacante exigirá un rescate a la víctima, normalmente en forma de moneda digital como Bitcoin, a cambio de la clave de descifrado que desbloquee los archivos cifrados.
5. Si la víctima paga el rescate, el atacante proporcionará la clave de descifrado y la víctima podrá acceder a sus archivos nuevamente. Sin embargo, no hay garantía de que el atacante realmente proporcione la clave, e incluso si lo hace, los archivos de la víctima pueden estar dañados como resultado del proceso de cifrado.

Es importante tener en cuenta que hay muchas variaciones en este proceso y no todos los ataques de ransomware seguirán estos pasos exactamente. Algunos ataques pueden no implicar el cifrado de archivos, por ejemplo, mientras que otros pueden implicar otras formas de extorsión o chantaje.

¿Cómo puedo sufrir un ataque de ransomware?

Hay varias formas de sufrir ransomware. Una de las formas más comunes es hacer clic en un enlace malicioso o archivo adjunto en un correo electrónico de phishing. Este tipo de correo electrónico está diseñado para parecer legítimo y a menudo parece provenir de una empresa u organización conocida. Al hacer clic en el enlace o archivo adjunto, el ransomware se instala en su ordenador. Otra forma de ser infectado con ransomware es visitar un sitio web comprometido. Estos sitios web han sido atacados por atacantes, quienes han insertado un código que instalará automáticamente el ransomware en su ordenador si visita el sitio. También puede recibir ransomware descargando archivos infectados de Internet. Esto puede suceder si descarga un archivo de un sitio web sospechoso o si descarga un archivo compartido por alguien que no conoce. En resumen, es importante tener cuidado al navegar por Internet y evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas. Esto puede ayudarlo a evitar sufrir ransomware y otros tipos de malware.

¿Quiénes son los objetivos de ataques de ransomware?

Los ataques de ransomware pueden dirigirse a cualquier persona que utilice un ordenador u otro dispositivo conectado a Internet. Sin embargo, algunos grupos tienen más posibilidades de ser víctimas que otros. Por ejemplo, los ataques de ransomware suelen dirigirse a las empresas, pues suelen tener datos más valiosos y pueden estar más dispuestas a pagar un rescate para recuperarlos. Los hospitales, las escuelas y otras organizaciones que proporcionan servicios críticos también son objetivos comunes, ya que un ataque de ransomware puede interrumpir sus operaciones y poner en riesgo la vida de las personas. Los ataques de ransomware también pueden dirigirse a los individuos. En estos casos, los atacantes pueden intentar extorsionar a la víctima para obtener dinero amenazando con eliminar sus archivos personales o publicar información confidencial, a menos que se pague un rescate. Los objetivos de los ataques de ransomware a menudo se seleccionan en función del valor de sus datos y su disposición a pagar un rescate para devolverlos.

¿Cuáles son los riesgos de pagar en un ataque de ransomware?

Pagar un rescate a un atacante de ransomware puede parecer la manera más fácil de recuperar los archivos, pero en realidad puede ser una decisión muy arriesgada. Existen varios riesgos asociados con el pago de un rescate, entre los que se incluyen los siguientes:

- No hay garantía de que el atacante realmente proporcione la clave de descifrado. En muchos casos, las víctimas que pagan el rescate nunca reciben la clave y no pueden acceder a sus archivos.
- Pagar el rescate puede alentar a los atacantes a continuar con su campaña de ataques. Si los atacantes saben que las víctimas están dispuestas a pagar el rescate, es más probable que realicen más ataques en el futuro.
- Pagar el rescate puede convertirlo en posible objetivo de futuros ataques. Si el atacante sabe que está dispuesto a pagar un rescate, será más probable que vuelva a ser objetivo.
- Pagar el rescate puede ser ilegal. En algunos casos, el pago de un rescate a una organización criminal puede considerarse una forma de financiación del terrorismo u otras actividades ilegales.

Si bien pagar el rescate puede parecer la manera más fácil de recuperar sus archivos, en realidad puede ser una decisión muy arriesgada. Es importante considerar con cautela los riesgos antes de tomar una decisión.

¿Cuál es el coste de un ataque de ransomware?

El coste de un ataque de ransomware puede variar en gran medida según una serie de factores, como el tipo de ransomware utilizado, la cantidad de archivos cifrados y la eficacia del ataque. En algunos casos, el coste de un ataque de ransomware puede ser relativamente bajo y los atacantes pueden exigir un rescate de unos cientos de dólares. En otros casos, el coste puede ser mucho mayor, ya que los atacantes exigen miles de dólares o incluso más para restablecer el acceso a los archivos de la víctima. Además de los costes directos asociados con el pago de un rescate, los ataques de ransomware también pueden tener costes indirectos significativos. Por ejemplo, un ataque de ransomware puede causar tiempo de inactividad y pérdida de productividad, lo que puede dar como resultado la pérdida de ingresos. También puede dañar la reputación de una empresa y la confianza del cliente, lo que puede tener consecuencias negativas a largo plazo para la empresa. Estos costes indirectos a menudo son mucho más altos que el rescate en sí mismo.

¿Cuáles son los síntomas de un ataque de ransomware?

Los síntomas de un ataque de ransomware pueden variar según el tipo específico de ransomware que se utilice. Algunos síntomas comunes incluyen los siguientes:

- Sus archivos están cifrados y no puede acceder a ellos.
- Recibe un mensaje del atacante que exige el pago de un rescate a cambio de la clave de descifrado.
- Ve programas o procesos desconocidos que se ejecutan en su ordenador.
- El ordenador se ralentiza o no responde.
- Su ordenador muestra mensajes de error inusuales o ventanas emergentes.

Si sospecha que su ordenador está infectado con ransomware, es importante actuar rápidamente. Desconecte el ordenador de Internet para evitar que el ransomware se propague.

Cómo evitar ataques de ransomware

Hay varias medidas que puede tomar para evitar los ataques de ransomware, entre ellas las siguientes:

- Utilice un antivirus o software de seguridad de confianza y manténgalo actualizado. Esto puede ayudar a proteger su ordenador contra ransomware y otros tipos de malware.
- Tenga cuidado al abrir archivos adjuntos o enlaces de correo electrónico. El ransomware a menudo se entrega a través de correos electrónicos de phishing, por lo que es importante tener cuidado con ser muy consciente de dónde se hace clic.
- Mantenga actualizado el sistema operativo y demás software. Las actualizaciones de software suelen incluir parches de seguridad que pueden ayudar a proteger el ordenador contra ransomware y otras amenazas.
- Haga copias de seguridad de los archivos con regularidad. Esto puede ayudar a proteger sus datos si el ordenador está infectado con ransomware. Asegúrese de adoptar una de las estrategias de copia de seguridad recomendadas, como la estrategia 3-2-1.
- Tenga en cuenta los riesgos del ransomware e informe a otras personas de su organización sobre estas amenazas. Esto puede ayudar a prevenir ataques de ransomware y facilitar la detección y respuesta si ocurren.

La mejor manera de prevenir los ataques de ransomware es permanecer alerta y tomar medidas para proteger el ordenador y los datos. Esto puede ayudar a reducir el riesgo de un ataque de ransomware y facilitar la recuperación de uno si ocurre.

¿Cómo puede Synology protegerme del ransomware?

Las acciones preventivas son esenciales para evitar convertirse en víctima del ransomware. Utilice estas soluciones de Synology además del software antivirus que elija:

- **Evitar el acceso**: reduzca la propagación del ransomware mediante la configuración de permisos de acceso, aplicaciones y archivos, y configure credenciales de inicio de sesión seguras mediante Secure SignIn y C2 Password.
- **Proteger los dispositivos**: los sistemas desfasados tienen un mayor riesgo. Actualice todos sus NAS a la vez con el Sistema de administración central (CMS) de Synology y proteja otros dispositivos con políticas de grupo en Synology Directory Server y C2 Identity.
- **Evitar archivos sospechosos**: los correos electrónicos de spam y phishing que contienen archivos sospechosos son métodos comunes para propagar ransomware. Synology MailPlus proporciona una sólida protección antimalware y prevención de spam.
- **Identificar vulnerabilidades**: utilice el Consejero de seguridad de Synology para buscar malware, vulnerabilidades y actividades de inicio de sesión anormales de forma rutinaria. Implemente los cambios recomendados para mejorar la seguridad de su NAS.
  https://www.synology.com/dsm/overview/security

Más formas de proteger sus datos

Administre su flota

Aproveche las amplias funciones para administrar centralmente los permisos de acceso a datos, el estado del software, el estado del sistema y mucho más.
https://www.synology.com/dsm/overview/administration

Monitorice todos sus sistemas

Identifique las actividades de inicio de sesión sospechosas, administre las actualizaciones y supervise el estado del dispositivo, sin importar dónde se encuentren sus dispositivos.
https://www.synology.com/dsm/feature/active-insight

Proteja sus datos

Siga la regla de copia de seguridad 3-2-1 para proteger sus datos contra modificaciones o eliminaciones accidentales y maliciosas.
https://www.synology.com/dsm/solution/data_backup

Primeros pasos

Contacto

Póngase en contacto con el departamento de ventas regional para obtener más información
https://www.synology.com/form/inquiry/sales

Dónde comprar

Buscar un socio de Synology en su región
https://www.synology.com/wheretobuy

Notas:

1. eSentire, informe sobre ciberdelincuencia oficial de 2022
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Proteja su organización contra el ransomware

https://www.synology.com/es-es/dsm/solution/ransomware

Sitio web de Synology

https://www.synology.com/

Contacte con nosotros

https://www.synology.com/company/contact_us