

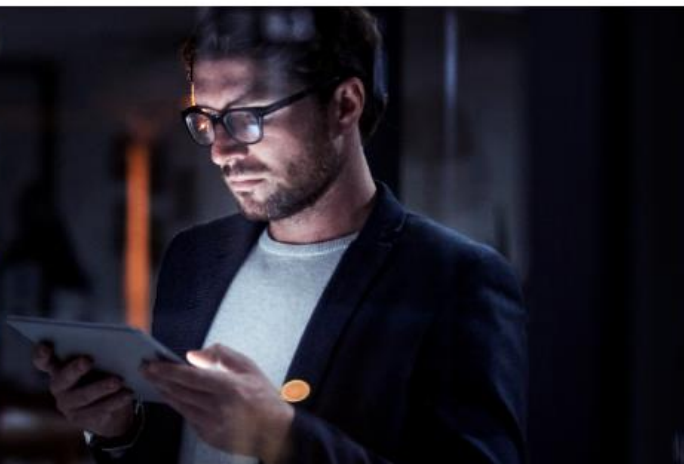


La seguridad es nuestra principal prioridad.

Las empresas se enfrentan al desafío de ofrecer un acceso seguro a una gama más amplia de servicios y aplicaciones, proporcionando al mismo tiempo protección frente a amenazas cada vez más sofisticadas. Synology ofrece soluciones de seguridad completas y mejoradas que le permiten adaptarse con mayor rapidez a las cambiantes tecnologías, las necesidades empresariales y las sofisticadas amenazas.

PSIRT de Synology

El Equipo de Respuesta a Incidentes de Seguridad de Productos de Synology (PSIRT) es responsable de la respuesta ante incidentes de seguridad de los productos de Synology. El PSIRT gestiona la recepción, la investigación, la coordinación y la presentación de informes públicos sobre vulnerabilidades de seguridad relacionadas con los productos de Synology.



Soluciones de recuperación proactivas

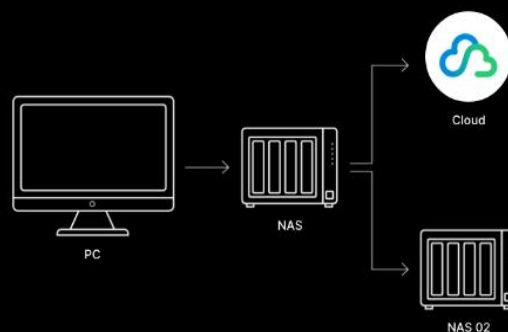
Existen varias formas de recuperar los datos si se ve afectado por amenazas como el ransomware basado en cifrado o daños físicos en el hardware.

Realice copias de seguridad externas

Métodos de recuperación proactivos

Realice una copia de seguridad en la nube

Haga una copia de seguridad de su ordenador en el NAS



Soluciones de recuperación proactivas

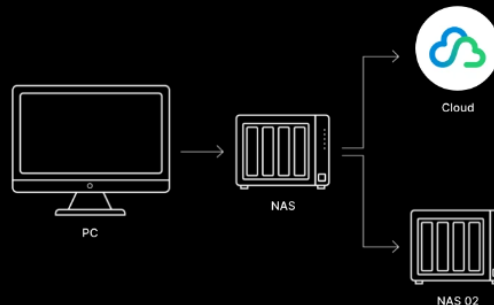
Existen varias formas de recuperar los datos si se ve afectado por amenazas como el ransomware basado en cifrado o daños físicos en el hardware.

Realice copias de seguridad externas

Realice una copia de seguridad en la nube

Refuerce su estrategia de seguridad con otro nivel de protección realizando una copia de seguridad de los datos del NAS en un dispositivo o NAS externo mediante Hyper Backup, Snapshot Replication y USB Copy de Synology. Se pueden configurar copias de seguridad de varias versiones, lo que ofrece más puntos de recuperación, mayor coherencia de los datos y eficacia de restauración.

Haga una copia de seguridad de su ordenador en el NAS



Rápida respuesta ante incidentes de seguridad

La seguridad es nuestra principal prioridad. Cuando recibimos el envío de una vulnerabilidad, realizamos una evaluación preliminar en un plazo de ocho horas y corregimos la vulnerabilidad en un día. Poco después de la confirmación, proporcionaremos un parche para garantizar la seguridad y la fiabilidad de todos nuestros productos.

8hr
INVESTIGACIÓN DE
VULNERABILIDADES

+

15hr
VULNERABILIDADES
CORREGIDAS

<

24hr
MANEJO RÁPIDO DE
EVENTOS



Mejoramos la seguridad junto con FIRST

El Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST) es la principal organización y es líder mundial en respuesta a incidentes. Como miembro del FIRST, el PSIRT de Synology puede responder a incidentes de seguridad de forma más eficaz, así como compartir su conocimiento del sector para ayudar a establecer estándares de seguridad más completos con socios líderes a nivel mundial.

Autoridad de asignación de CVE

Synology ha recibido por parte de MITRE Corporation, un instituto de seguridad de reconocimiento internacional, la autorización para ejercer como una CNA (autoridad de asignación de CVE). Gracias a nuestra capacidad para asignar ID de CVE a las vulnerabilidades que afectan a nuestros productos, podemos reforzar nuestro compromiso por avanzar con nuestras soluciones de seguridad.



Por medio de los programas de recompensa, nos comprometemos con la comunidad hacker.

En Synology, nos esforzamos por crear productos seguros para proteger la información de los usuarios. Cada año, invitamos a los principales hackers e investigadores de seguridad externos a contribuir a la mejora del perfil de seguridad de nuestros productos a través de programas de recompensas de hasta \$20000 USD. También participamos en concursos de piratería como Pwn2Own y TienFuCup para permitir que los equipos de hackers verifiquen nuestras medidas de seguridad. Nuestros equipos de desarrollo se comprometen a publicar soluciones para los problemas críticos y relacionados con el sistema operativo en un plazo de 60 días.



Política de respuesta a vulnerabilidades de Synology

En este documento se describe el enfoque de Synology para la aplicación de seguridad y cumplimiento de directivas para Synology DiskStation Manager (DSM).

[Obtener más información](#)

Auto-protección contra ransomware

Consciente del auge del malware, Synology introduce potentes medidas de seguridad, como Snapshot Replication o la figura del consejero de seguridad, y ofrece actualizaciones periódicas para defender a los usuarios de las amenazas potenciales.

[Obtener más información](#)

Asesoramiento de seguridad de los productos de Synology

Empresa dedicada a la seguridad del cliente y a la seguridad continua en todos nuestros productos, Synology aplica medidas inmediatas cuando detecta posibles vulnerabilidades tras la realización de alguna prueba interna, como resultado de una investigación o cuando recibe la información directamente de los clientes.

[Obtener más información](#)

Seguridad de DSM

DSM ofrece avanzadas medidas de seguridad para la protección de empresas contra ataques maliciosos, ya que garantiza la seguridad de los activos digitales críticos y la total ausencia de tiempo de inactividad por problemas de este tipo.

[Obtener más información](#)

