

QNAP

Cyber Security

Cómo garantizar una recuperación rápida y protección contra ransomware para copias de seguridad de datos NAS empresariales

En el desafortunado caso de un ataque de ransomware, los usuarios normalmente se dan cuenta del problema sólo después de que los datos de su sistema principal han sido cifrados, lo que les solicita que restauren desde una copia de seguridad. Sin embargo, si los datos de la copia de seguridad también están cifrados, la recuperación se vuelve imposible. Es por eso que las copias de seguridad se deben almacenar de forma segura en un entorno aislado.

QNAP ofrece una variedad de soluciones Air Gap para ayudar a los clientes a proteger sus datos de respaldo de amenazas de ransomware.

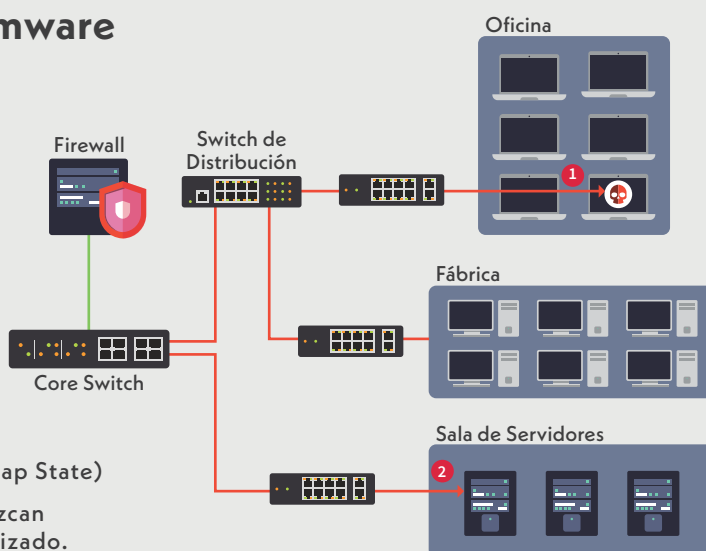
Cómo ocurren los ataques de ransomware

El ransomware se infiltra en las organizaciones a través de dispositivos no seguros, generalmente cuando un empleado abre un archivo adjunto de correo electrónico malicioso o conecta una unidad USB infectada.

Una vez dentro de la red, el ransomware intenta propagarse a otros dispositivos con privilegios elevados, incluidos servidores de archivos y sistemas MES.

→ Los datos críticos deben estar en un "estado aislado" (Air-Gap State)

=Esto significa garantizar que los datos importantes permanezcan inaccesibles a través de la red, lo que evita el acceso no autorizado.



Puntos clave para la protección contra ransomware

¿Qué es Air Gap?

Air Gap es un entorno físicamente aislado que impide que el ransomware acceda a los datos de respaldo.



- Almacenamiento fuera de línea, como copias de seguridad en cinta
- Almacenamiento completamente separado, desconectado de servidores y redes

Dado que el ransomware solo puede infectar dispositivos conectados a la red, **almacenar copias de seguridad de seguridad en un entorno sin conexión** es una de las contramedidas más eficaces.

Este método, conocido como "**air-gapping**" o "**backup aislado**", garantiza que el ransomware no pueda detectar ni cifrar los datos de la copia de seguridad, manteniéndolos seguros.

Soluciones de respaldo Air-Gap disponibles con QNAP NAS

Soluciones de Backup con Air-Gap de QNAP

QNAP ofrece tres **soluciones de respaldo con Air-Gap**, lo que permite a los usuarios elegir la mejor opción según la importancia de los datos y el presupuesto.

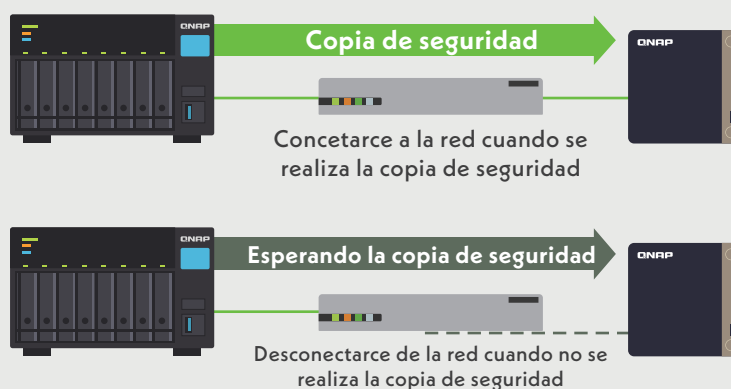
Backup mediante USB Air-Gap

El NAS de QNAP admite **dispositivos de almacenamiento conectados por USB** a través de puertos USB. Al configurar el dispositivo USB como una **unidad de red invisible** y establecer permisos de acceso para denegar todo acceso, el disco permanece oculto e inaccesible. Realizar una copia de seguridad de los datos del NAS en el dispositivo USB garantiza la protección contra amenazas de ransomware.



Backup AirGap+

La **solución de copia de seguridad AirGap+** de QNAP funciona con routers QHora y se conecta a la red **solo durante las copias de seguridad programadas**. Cuando no se utiliza, la red permanece desconectada, lo que reduce significativamente el riesgo de infección por ransomware.



Backup LTO

QNAP ofrece **soluciones de copia de seguridad en cinta LTO** para el archivado de datos a largo plazo. Las cintas LTO ofrecen una **longevidad de almacenamiento de más de 30 años** y se pueden extraer físicamente y almacenar sin conexión, lo que las hace **completamente inmunes a los ataques de ransomware**. Esta solución es ideal para el **almacenamiento a largo plazo basado en el cumplimiento** normativo y el transporte de copias de seguridad **fuera del sitio**.

QNAP SYSTEMS, INC.

Copyright © 2025 QNAP Systems, Inc. All rights reserved.

www.qnap.com