Ransomware prevention and protection by Synology

By Olga Papadimitriou – Business Development Officer

Sophisticated Ransomware and other malware threats are increasing so fast that business and home internet users are in a constant threat for becoming victims and pay significant amount of money to gain access to their own data, or prevent any deletion, selling, or further leak of data.

Research showed that

- **$20 billion** in total global damage is caused by ransomware attacks annually
- **11 seconds** is the time it takes for another business to be attacked
- **304 million** ransomware attacks were reported in 2020, a 62% yearly rise

To protect your data against threat actions, it is essential take preventative actions.

Synology, to protect and restore data, provides products with prevention and recovery solutions which you can combine with antivirus software of your choice:

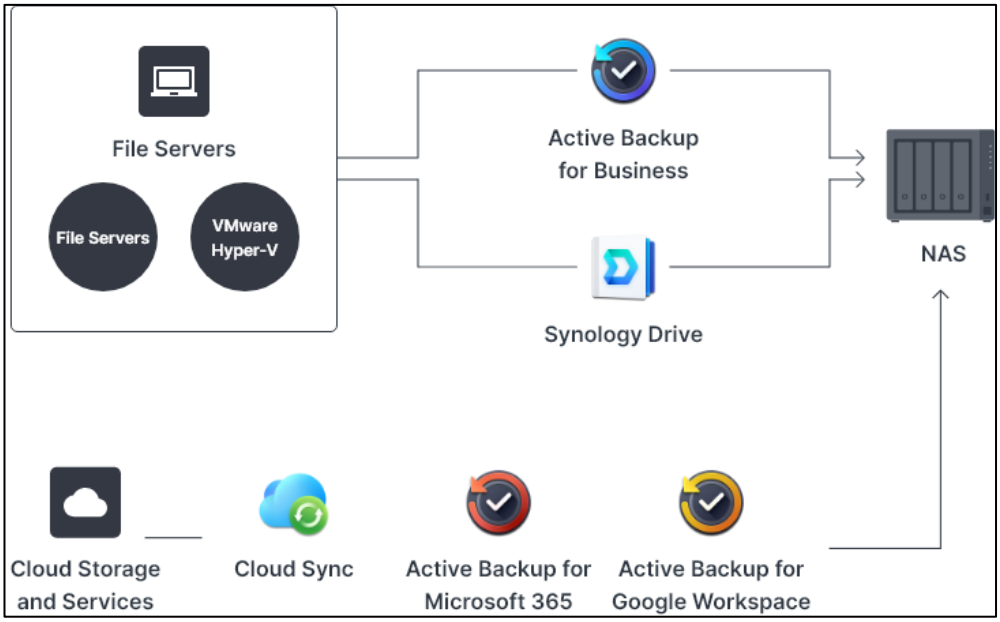
- **To Prevent access and reduce the spread of ransomware:** Set file, application, and access permissions, and configure secure login credentials using Synology **DiskStation Manager (DSM)** to shield your data against unauthorized access and **C2 Password** to store all your credentials in one place securely.
- **To Protect devices:** Update all your NAS at once with **Synology CMS**, and safeguard other devices using group policies in **Synology Directory Server** and **C2 Identity**.
- **To Avoid suspicious files:** Spam and phishing emails containing suspicious files are common methods of spreading ransomware. **Synology MailPlus** provides strong anti-malware protection and spam prevention.
- **Check for vulnerabilities:** Use **Synology Security Advisor** to routinely scan for malware, system vulnerabilities, and abnormal login activities. Implement recommended changes to improve your NAS security.

How to recover from a ransomware attack

Having backups of your data can reduce the damage caused if you've been a victim of a ransomware attack. Synology NAS with its robust backup features can help you continue operations

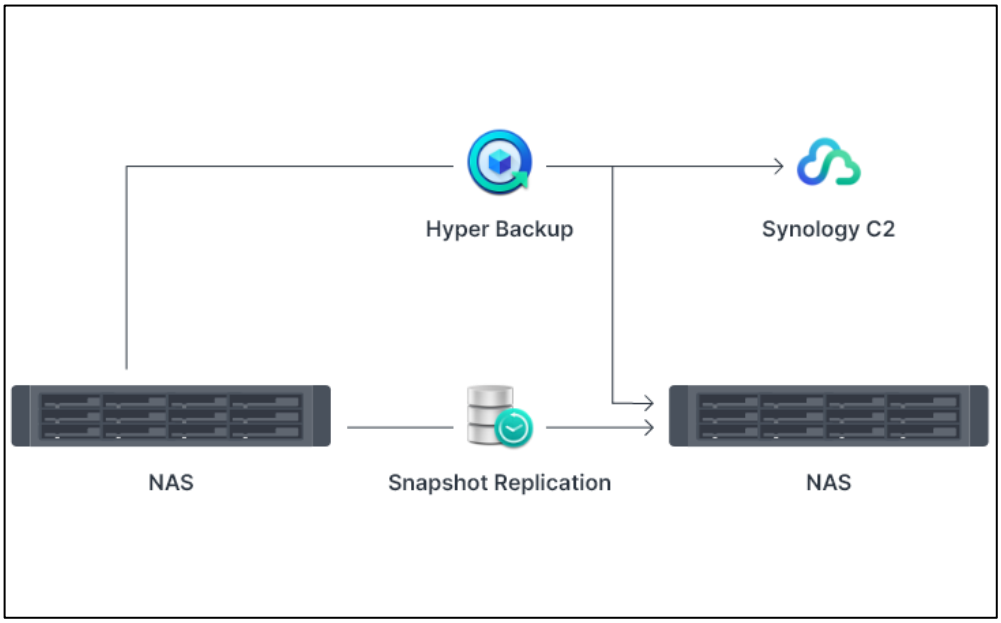
with minimal disruption. Note that, before restoring backups, it is important to make sure your device has been cleaned.

1. **Back up to your NAS.** Synology NAS is perfectly suited as a backup location for all your digital assets.
    - **Safeguard important files.** Set up real-time versioning or scheduled backups to avoid getting locked out of your files and folders. NAS can retain up to 32 previous versions of files from any computer to keep them safe from folder encryption.
    - **Protect entire systems.** Backup your deployments to your NAS to prevent threat actors from holding them for ransom. Backing up data from physical computers, virtual environments, or SaaS applications to your NAS is an easy action.
    - **Synchronize cloud-based data.** It is mandatory to keep an updated copy of your public cloud-hosted files on a Synology NAS. Your data can be encrypted on your NAS to keep them safe if your public cloud service becomes compromised or inaccessible.



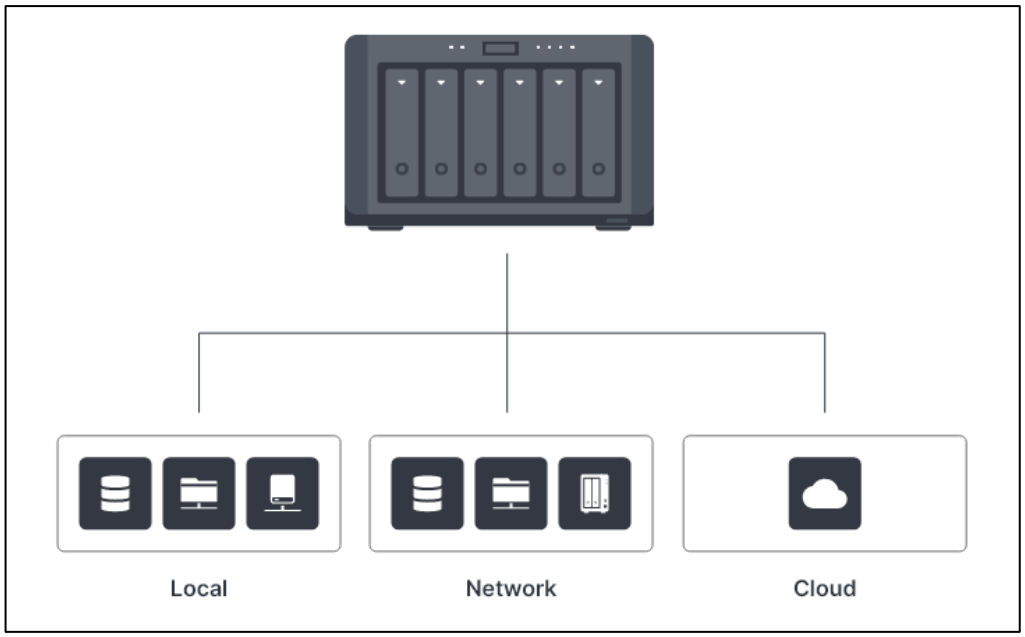
2. **Back up off-site.** Keep copies of your files and restore them if you are affected by ransomware.
    - **Leverage another NAS.** Take snapshots of shared folders or LUNs and replicating them to another Synology NAS to defend against ransomware attacks.

- **Store data on an external device.** Copy your NAS data and configurations to a separate device for safekeeping. Back up your NAS to remote servers or cloud destinations with powerful customization options to reduce storage usage and protect data against unauthorized access.
- **Keep a cloud copy.** Retain unlimited backup copies that are encrypted and stored in a secure cloud infrastructure powered by Synology to protect individual objects, entire on-premises devices, and NAS data and configurations.



3. **Restore your backups.** You can recover your data and applications by restoring your backups from a NAS or an off-site location even if your devices have been compromised.
    - **Take back your files and folders. Snapshot Replication** allows you to quickly restore access to LUNs and shared folders on a primary NAS or fail over to another NAS in seconds. With Synology Drive Client you can restore from NAS previous versions of files stored on computers.
    - **Regain your system.** Active Backup for Business allows you to recover PCs, servers, and virtual machines to a previous clean state using backups on your NAS if any of your endpoints are compromised. With Hyper Backup you can also fully restore your NAS from an off-site backup.

- **Recover with the cloud.** Cloud backups are a safe and secure location to retrieve data from because they are not directly connected to compromised on-premises devices. You
- can restore entire PCs or individual files with **C2 Backup** while you store your copies of Synology NAS files and system configurations for fast and reliable recovery with **C2 Storage for Hyper Backup.**



Reduce threat risk and protect your data

Having an effective data protection solution can reduce the risk of being locked out of vital data. Synology with its complete collection of data protection solutions, secures home and work environments from data loss.

IBSCY Ltd is a certified provider of Synology NAS in Cyprus, and it has the knowledge and experience to sell, install, and maintain all its products. IBSCY is an expert provider of total IT products and IT services, and it specializes in designing sophisticated solutions to complicated problems using technology and making sure that all your vital data are secured from any threats so that your business processes can run seamlessly.