

NETWORK ATTACHED STORAGE

SYNOLOGY BUSINESS NAS SOLUTION

STORE AND PROTECT YOUR IMPORTANT DATA USING A SYNOLOGY NAS SOLUTION

Small and Medium-size businesses rely on their data to constantly be available

PURPOSE / INSTRUCTIONS

The heart of a small or medium-sized information technology footprint is their data. Data loss or corruption can lead to serious consequences. The imperative is to protect data so that it is available 24x7. Safe Computing can recommend a Synology solution that best fits your business requirements.

A Synology NAS becomes a powerful, resilient storage platform when hardened properly and paired with a second device for immutable, off-site backups. Modern DSM versions (7.2+) introduce enterprise-grade protections such as Btrfs snapshots, WORM immutability, and snapshot replication, which together create a strong defense against ransomware, accidental deletion, and insider threats.

Core Functions of a Single Synology NAS

A single Synology NAS provides centralized, fault-tolerant storage with built-in data protection features. Its baseline capabilities form the foundation for a secure backup strategy.

Storage & File Services

- Shared folders, SMB/NFS/AFP file services
- Btrfs or ext4 volumes, with Btrfs enabling advanced protections
- User/group permissions and access control

Local Data Protection

- **Snapshots:** Near-instant, point-in-time copies using Btrfs copy-on-write. They consume minimal space and allow rapid restoration of files or entire folders.
- **Immutable Snapshots (WORM):** DSM 7.2+ allows snapshots to be locked for a defined retention period, preventing deletion or modification—even by administrators.
- **Self-service recovery:** Users can restore files from the #snapshot directory without admin intervention.

Security & Ransomware Resistance

- Built-in protections against tampering and accidental deletion
- Snapshot schedules with GFS-style retention (hourly/daily/weekly) recommended for resilience
- Rapid rollback of corrupted or encrypted data

SAFE COMPUTING | Cybersecurity for Small Business

safe-computing.net • info@safe-computing.net • 512.228.0411 • 213 Bluff St, Buda, TX 78610

Management & Automation

- Snapshot Replication package for scheduling, retention, and protection policies
- Automated snapshot creation and expiration
- Quick restore workflows for folders, LUNs, or individual files

Added Value of a Two-NAS Setup

Using two Synology NAS devices—one local and one remote—dramatically increases resilience. This architecture supports true off-site protection and immutable backup replication.

Remote Snapshot Replication

Synology's Snapshot Replication app allows you to replicate snapshots from NAS A (primary) to NAS B (remote).

- Replication tasks can be scheduled (hourly/daily)
- Remote snapshots can be made **immutable**, preventing deletion for 7–14 days or longer
- Even if the primary NAS is compromised, the remote immutable snapshots remain untouched

Immutable Remote Backups

Immutable remote snapshots provide ransomware-resistant, disaster-proof backup copies.

- WORM protection ensures snapshots cannot be altered or deleted until the retention period expires
- Storage spaces containing immutable snapshots cannot be deleted, adding another layer of protection
- Attackers cannot encrypt or remove remote snapshots, even with stolen admin credentials

Enterprise-Grade Resilience

With two devices, you gain:

- **Geographic redundancy** (fire, flood, theft protection)
- **Ransomware-proof restore points**
- **Regulatory retention compliance** (WORM retention windows)
- **Fast recovery** from either local or remote snapshots, depending on the incident type

Typical Workflow

1. Install Snapshot Replication on both NAS devices.
2. Configure snapshot schedules on the primary NAS.
3. Create a replication task targeting the remote NAS.

SAFE COMPUTING | Cybersecurity for Small Business

safe-computing.net • info@safe-computing.net • 512.228.0411 • 213 Bluff St, Buda, TX 78610

4. Enable **immutable snapshots** and set a retention period (7–14 days recommended).
5. Periodically test restoration from both local and remote snapshots.

■ Conclusion

A single Synology NAS provides strong local protection through Btrfs snapshots, immutability, and efficient recovery tools. But pairing two NAS devices unlocks true enterprise-grade resilience: immutable remote backups, off-site protection, and hardened defenses against ransomware and accidental deletion. DSM 7.2's WORM snapshot features ensure that even compromised administrators cannot destroy your last line of defense.

This two-device architecture transforms Synology from a simple NAS into a robust, multi-layered data protection system suitable for both home labs and business environments.