Synology®

C2 Storage Data Encryption and Durability Strategy

Last updated: Feb 10, 2023

Table of Contents

Executive Summary

Businesses need to prevent loss of their valuable data due to human mistakes, hardware failure, or degradation. This necessitates a backup strategy. At the same time, they need to prevent data breaches of live and backed up data due to unauthorized access, unintended leaks, and malicious attacks. Storing large pools of data in different places and protecting access to sensitive information may seem to clash. Sometimes, the answer is in the cloud.

Synology C2 Storage offers Synology NAS users a tool to ensure data availability on the cloud to prevent data loss due to human error and disasters, and ensure business continuity at all times. Synology's security features help Synology C2 Storage users achieve data security by restricting access through advanced technologies, wherever the data are located. With C2 Storage, safety need not come at the price of security.

Introduction

Remote cloud storage is increasingly recognized as an essential component of strategies to prevent permanent or temporary data loss—a threat that can cost businesses as much as, or more than malicious theft and accidental leaks. C2 Storage gives Synology users access to a powerful cloud solution for data protection.

Causes of Network-Wide Data Loss

Many businesses execute regular backups to remote NAS or other servers. These are excellent protections against the most common causes of data loss. However, it can never be excluded that issues affecting one device can wreak havoc on a company's whole infrastructure.

In its 2019 Internet Security Threat Report, Symantec reported a 12% rise the previous year in ransomware attacks on companies, in which data are kept hostage. Among attacks embedded in trusted software (up 78%), it registered a 25% rise in those that purely destroyed data and IT infrastructure. The network-wide scope of such attacks can slow down recovery efforts and threaten multiple backup locations.

The US-based Disaster Recovery Preparedness Council in a widely-cited 2014 study found entrepreneurs unprepared for outages and data loss due to hard- and software failures, human error, power failure, and natural disaster.

In case of sudden loss, most businesses had backup and restoration plans that included storing backups on a second device. However, it often took too long for critical applications and records to come back online. Many data were never recovered due to missed backup points, for instance due to switched-off devices.

Adopting Multi-Pronged Backup Strategies

It can pay off for businesses to keep copies of their essential applications and records not only safely stored, but also quickly accessible from anywhere by leveraging the cloud.

An increasing number of businesses employ a "3-2-1 backup strategy" for their data protection plan: They maintain three copies of backed-up data, of which two are stored on different media and one is hosted offsite. The offsite copy is often kept in the cloud.

Creating a "3-2-1" Backup Strategy With Synology

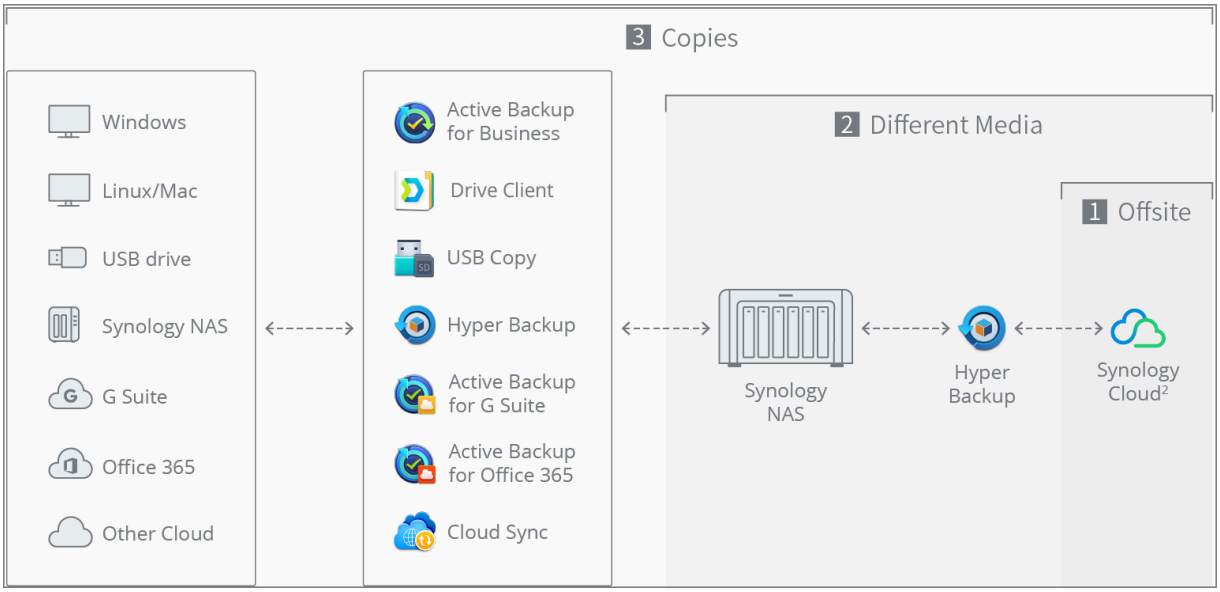

Figure 1: Synology provides a host of methods to back up data to Synology NAS. To protect against local disaster, cyberattacks, or IT failure, remote copies of backups can be stored to the cloud with C2 Storage, completing a "3-2-1 backup strategy."

Synology's Solution for Offsite Backup

Synology offers users cloud storage tailored for backup use that matches reliability with security. Synology's C2 Storage is a safe cloud backup solution for Synology NAS users fully integrated with Synology Hyper Backup.

Synology C2 Storage provides safe offsite data storage, as well as full protection during the processes of backing up, transferring, preserving, and restoring data. Data security is achieved through multiple layers of encryption during transmission, as well as storage.

Full integration with Hyper Backup makes it easy to restore full versions from the internet, as well as individual files. The Synology C2 Storage web portal allows users to access and restore files anytime, anywhere, for maximum speed of recovery. Location-independent backup restoration helps you get your projects up-and-running faster after data-loss events.

This paper explains the technologies Synology employs to keep data both secure and safe, and suggests how Synology C2 Storage users can improve their data security setup with just a few easy steps.

Data Encryption

When using Hyper Backup to transmit data from Synology NAS to Synology C2 Storage, Synology strongly recommends that users enable client-side encryption for breach prevention. This section details Synology's data protection and encryption methods for users combining Hyper Backup with Synology C2.

Concerns About Security in the Cloud

Security concerns might deter risk-conscious entrepreneurs from taking the next step toward guaranteeing the availability of their data. Backups stored on private servers may intuitively feel safer.

However, with the protection technologies available today, there is no reason that information stored in well-protected data centers should fall into unauthorized possession. Encryption can protect leaked files from abuse by rendering the data unreadable in the wrong hands.

In a 2019 report for digital security firm Gemalto, encryption was the most widely mentioned prevention measure considered by companies in response to data breaches. However, the complexity of implementation across applications and environments was listed as the greatest obstacle to wider adoption.

Using Synology C2 Storage with Synology Hyper Backup can help businesses centralize implementation and management of their data protection strategy, taking away a major hurdle to cloud-based backup storage.

Ensuring Protection at Every Stage

Hyper Backup performs client-side encryption during backup, making data unreadable before they leave the server or network. Synology employs the AES-256 encryption standard for data transmission and storage.

When a backup task is created, data are processed into 50MB data chunks, which are individually encrypted using AES-256. A new random (symmetric) key is generated for each stored version.

Keys are in turn encrypted using the RSA-2048 iteration of the (asymmetric) RSA cryptosystem to ensure their secrecy. This process yields a public key, which is stored on users' Synology NAS and Synology C2 Storage, and a private key, which can be downloaded to PCs and personal devices. Data are thus protected by two layers of encryption.

Backed-up data can only be viewed or restored when the public and private keys are matched. Without the private key, all data are unreadable. In addition to content, AES-256 encryption is separately applied to file names, using a version-independent, permanent symmetric key.

Encryption-at-Rest

Customers have the possibility of not enabling client-side encryption. However, Synology protects all data on its servers against breach or physical theft with encryption-at-rest. Like user data, C2 Storage servers and drives are encrypted up to the AES-256 standard, with a key kept on another system, ensuring that no device can be read out by unauthorized actors.

Secure Transmissions with SSL

Communication between Synology NAS and Synology C2 servers happens using SSL protocol, which ensures encryption, authentication and integrity checks. This means that both the backup data and the connection are encrypted.

Like Synology's data protections, the SSL protocol prevents data from being modified or corrupted during transmission through a combination of symmetric, shared-key encryption of data and asymmetric, public-key cryptography for the initial "handshake."

Client-Side Encryption and Transmission

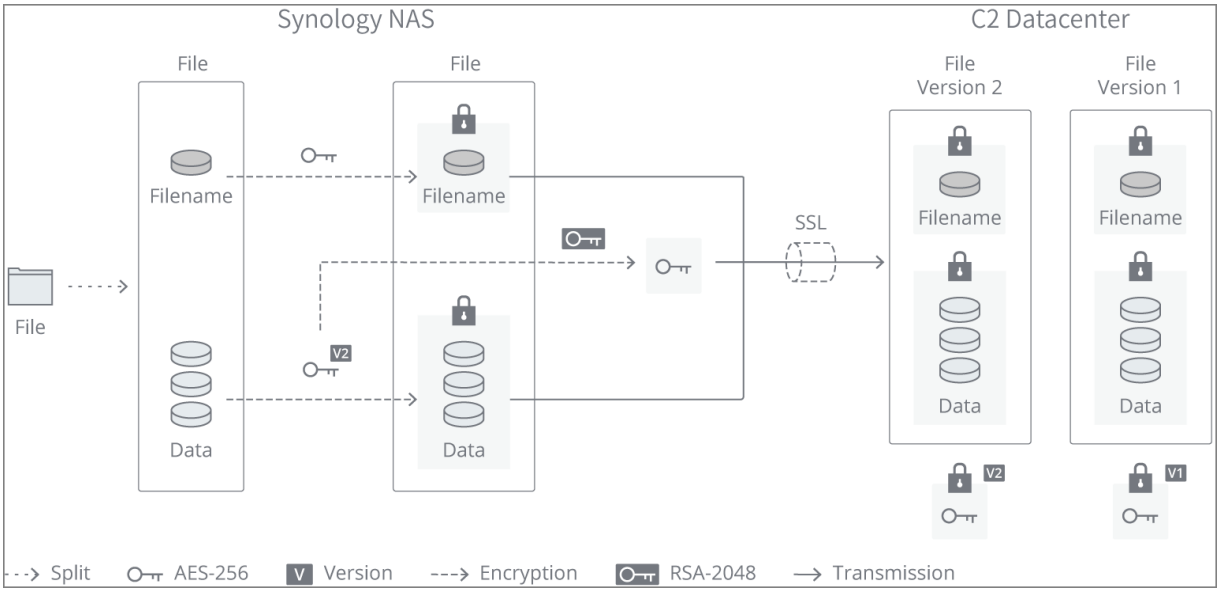

Figure 2: AES-256 client-side encryption of data chunks yields an AES key, which is encrypted with RSA-2048 and stored on the server. Cloud storage providers are not only expected to prevent unauthorized access to private files, but also to guarantee that data are continuously available and remain in top shape over long periods of time.

Data Durability

Cloud storage providers are not only expected to prevent unauthorized access to private files, but also to guarantee that data are continuously available and remain in top shape over long periods of time.

Users must be able to retrieve the files at a moment's notice, free of any data errors, even after years of storage. The ability to keep stored data consistent and intact, without the influence of bit rot, drive failures, or any form of corruption, is called durability.

Many cloud storage providers list a number of "nines" of durability. Synology follows procedures preferred by industry leaders to offer an estimated "nine nines" (99.9999999%) to "twelve nines" of data durability according to widely-used definitions. The protection provided exceeds that of available RAID configurations.

For a critical discussion of the calculation and use of this statistic, refer to this blog about data durability by our research and development staff.

Fault-Tolerant Storage

Synology C2 data center architecture ensures that no valuable data is lost. Highly available and redundant infrastructure minimizes risks by physically eliminating so-called "single points of failure." This means parallel systems stand ready to take over if the main configuration experiences downtime.

Meanwhile, strategic policies and coding measures prevent data loss or corruption if hardware failures nevertheless occur.

Erasure Coding for Data Durability

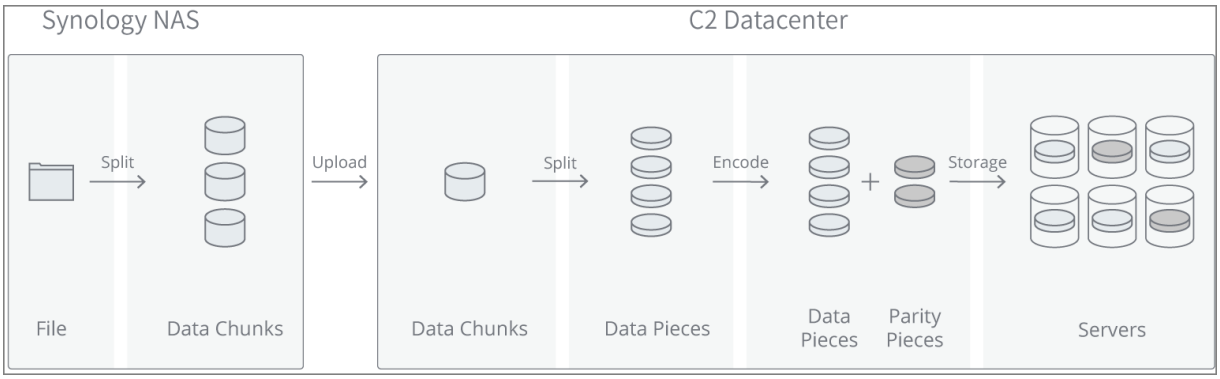

Figure 3: Data uploaded to C2 servers are split into pieces and encoded, generating parity pieces that keep data retrievable when one ore more servers are down.

Synology employs erasure coding, the gold standard in data durability technologies, to safeguard data integrity in the face of server crashes, drive failures, and writing errors. Erasure coding takes a similar approach to most RAID configurations by relying on smart distribution with redundant data to enable checks and recovery.

Hyper Backup divides files selected for backup into data chunks of about 50 MB for upload. After encryption and transmission (as well as optional compression and deduplication) each chunk is distributed over several data pieces hosted on as many discrete servers.

Several pieces out of each set are redundant, so that a number of servers, drives, or pieces may be lost or damaged at any time without compromising the ability to retrieve the original chunk or to check its integrity. The configurations used reduce the likelihood of such events to many digits behind the decimal point, or practical impossibility.

Bit rot can also be detected. When data is written to the hard drive, the storage service calculates the MD5 checksum and records it in the extended file attributes, which allow users to correlate computer files with metadata that the file system has not yet processed. When the storage service reads the data, the MD5 checksum will be re-calculated and will check for any abnormalities with the MD5 checksum recorded on extended file attributes. If any data has detected abnormalities, it will be quarantined, and the redundant and healthy data will be used to recover the data set.

Synology’s Erasure Coding Setup

Synology employs erasure coding setups that ensure at least three pieces of redundancy. This means that if each data chunk is distributed over 15 pieces on 15 nodes, only 12 of these are needed to reconstruct any file.

In other words, up to three devices or pieces can be compromised without users losing access. Hardware-level failures, if they occur, are thus highly unlikely to affect Synology C2 data.

In the above example, any file can be reconstructed from any combination of 12 data pieces. This means Synology’s cloud storage setup offers significantly higher redundancy than RAID 5 configurations (1 disk redundancy) or RAID 6 storage setups (which can tolerate 2 broken disks).

Unlike with RAID configurations, which need time to rebuild following failure, recovery of files in C2 Storage's erasure-coded setup is fast and painless.

Accessing the Cloud

Good key and password management is essential to protect your own access to data, account details, and settings while keeping out unwanted intruders. Reviewing the different ways to access C2 Storage can help users make informed decisions on which services to use and which access options to enable.

Storing Private Keys

When setting a backup task with client-side encryption in Hyper Backup, users are prompted to download the private key for the task. Keys can be stored as files on personal devices and uploaded to decrypt RSA-protected data in case users forget their passwords.

Synology strongly recommends saving private keys in a secure location for each task. Without a private key, users will permanently lose access to their files when they forget their password. A separate private key is generated and can be stored for each task.

A password-protected copy of each private key is stored on Synology C2 servers and is accessible only with the password set for the specific backup task. This task password allows client devices to download and decrypt the hash-protected private key.

Setting up 2-Step Verification

Synology NAS users can set up 2-step verification for their Synology Account and DSM user accounts. When enabled, a time-dependent verification code displayed on the user's mobile device must be entered to sign in to DSM.

Enabling 2-step verification in DSM protects access to Synology C2 via Synology NAS servers. Users can separately enable 2-step authentication for their Synology Account to protect direct logins to Synology C2. Please refer to this article for more information.

Retrieving Data and Client-Side Decryption

Users can restore or download backups to their Synology NAS using Hyper Backup in DSM, or to their Windows, Linux and Mac computers using Hyper Backup Explorer. Retrieving data requires both user account and encryption key verification. In this case, decryption is applied at the client side.

Signing into user accounts requires password authentication and use of a 2-step verification app, if enabled. Encryption keys are verified either with a separate encryption password set for the

backup task, or with the original private key file.

Users have a choice of downloading individual files, or an entire backup image (only to Synology NAS). They can also decide whether to save backup data separately, or to replace damaged data with recovery files.

Retrieving Data and Client-Side Decryption

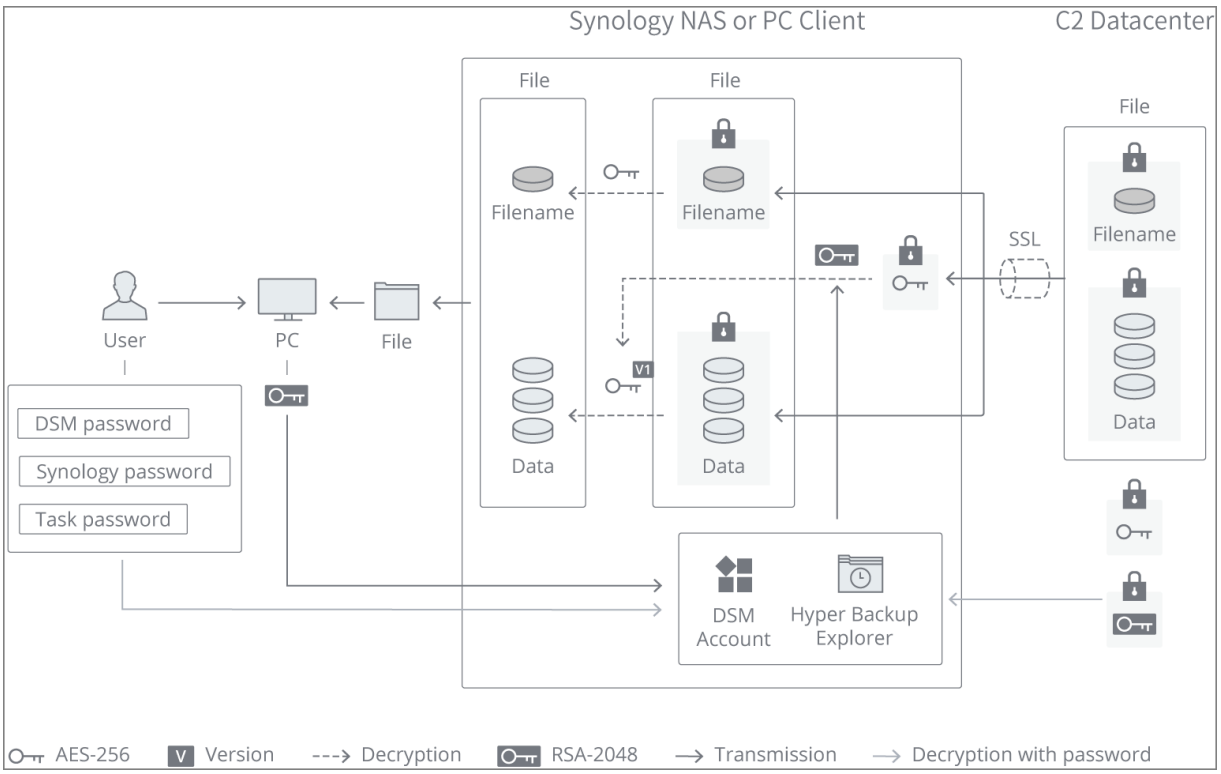

Figure 4: Users are advised to store RSA private keys to a personal device. Importing RSA keys to Hyper Backup Explorer or Synology NAS is the recommended way to decrypt files. However, users can also unlock RSA keys with a password set separately for each task.

Web-Based Retrieval Option

As an alternative, users who cannot perform client-side decryption may retrieve individual backed up files using the Synology C2 Storage online portal. If enabled, the portal allows users to sign in and upload a private encryption key or enter a task password to start decryption of their data.

Only individual files can be retrieved from the portal, and data are sent over an encrypted SSL connection. However, for the most secure experience, we recommend decryption using Hyper Backup and Hyper Backup Explorer.

Service Termination

Upon termination of a Synology C2 subscription, users lose access to their remotely stored data. This does not affect their right to data protection. Synology safely removes user data from its servers immediately after termination of the service, ensuring that neither the user nor cybercriminals can gain access.

Data Centers

Physical Location

We currently exclusively operate data centers worldwide. For more information about our data center location, please visit our official website. All users are ensured that their data is hosted in each location. For example, our EU-based data center allows business customers to comply with European data protection laws. New locations may be added in the future. However, this will not affect existing clients or their data.

Please see our Synology C2 Services terms and conditions and Data Processing Agreement for more details on legal guarantees.

Site Security

Synology data centers have passed rigorous inspections for strict security procedures and physical safety features, and meet Synology's high standards for incident response and access restrictions. Synology monitors employee access to its storage locations.

Security Incident Response

In-House Expertise

Synology's in-house Product Security Incident Response Team (PSIRT) is tasked with handling security incidents affecting Synology products. They receive and investigate reported vulnerabilities, coordinate responses, and publish information on security vulnerabilities that affect Synology products.

Our security researchers conduct periodic reviews of potential vulnerabilities in existing products, providing suggestions and alternatives for better security services. Upon detection of a vulnerability, a preliminary assessment is made within eight hours and a fix is provided within one day. A patch will be made available within a short period of time.

Bounty Program

Synology has been running a public Security Bug Bounty Program since 2017. Security researchers from around the world are invited to help enhance product security.

Synology accepts vulnerability reports related to its products and web services from researchers, offering monetary rewards to those who identify potential vulnerabilities and listing their names on its Security Advisory page.

Conclusion

Synology C2 Storage offers Synology NAS users a tool to ensure data availability on the cloud, to prevent data loss due to human error and disasters, and ensure business continuity at all times. Synology puts security and privacy first when designing its services, giving customers full control over their data, even in the public cloud.

Synology C2 follows industry best practices by encrypting data during storage and transmission using two global standards. Meanwhile, data is kept consistent and intact using an erasure coding approach to data durability in concert with physical redundancy and high-availability infrastructure.

In combination with Hyper Backup integration, that makes Synology C2 the best and most convenient option for Synology NAS users who want to take data protection to the next level using cloud-hosted copies of their essential backups without compromising on safety.