Retrospect

# Backup for Small Businesses

# Retrospect Backup vs NAS File Sharing

Pick the right tool to protect your business.

## The Best Tool for the Job

### System Recovery

File sharing syncs files. It does not protect your operating system. It takes days to recreate an operating system from scratch, with specific operating system versions, system state, application installations and settings, and user preferences. You cannot restore these from the file share. Retrospect does full system backup and recovery for your entire environment.

### Cloud Backup

Theft and disaster have always been important reasons for offsite backups, but now, ransomware is the most powerful. Ransomware will encrypt the file share just like any other file. Retrospect integrates with over a dozen cloud storage providers for offsite backups, connects securely to prevent access from malware and ransomware, and lets you transfer local backups to it in a couple clicks.

### File and System Migration

Retrospect offers built-in migration for files, folders, or entire bootable systems, including extended attributes and ACLs, with extensive options for which files to replace if source and destination overlap. Every file is an exact clone, down to the byte.

### Powerful Filtering

File sharing only synchronizes the files in the shared folder. With Retrospect, you can protect your entire system or any subset of it. It has a powerful set of filters available, with inclusion and exclusion logic, to ensure you can back up only critical data (like documents) and ignore non-business areas (like your movie library).

### Complete Data Protection

With cross platform support for Windows, Mac, and Linux, Retrospect offers business backup with system recovery, local backup, long-term retention, along with centralized management, end-to-end security, email protection, and extensive customization–all at an affordable price for a small business.

## 3 Ways for File Sharing to Fail

Network-attached storage (NAS) devices are an affordable, on-site solution for file sharing. Files can be easily stored on the share and mounted on Windows, Mac, and Linux computers. Because the NAS is on-site, files do not need to be synced down from a cloud service. Drop a file into file share folder, and you're good to go, for that file. Unless something happens.

### 1) No Disaster Recovery

All hardware eventually stops working, but you never know when. One morning, your computer just does not turn on. You can sync your file share folder to a new computer, but everything that was not on the file share is gone. Downtime is costly, and you don't want to spend days recreating your system, bit by bit. You want to get back to work.

### 2) Ransomware Strikes

Ransomware affects individuals, small offices and large companies. Anyone at any business can get an email from UPS with a PDF attached, double-click on it without thinking, and infect their computer with ransomware. Getting your data back only costs $500, unless it costs more or the decryption feature is buggy or there was never a decryption feature. Your entire computer is not on the file share. What data are you going to miss when ransomware hits?

### 3) File Not Shared

Shared files live in a specific shared folder. If your file is not in that folder, the file is not protected, and it's easy to forget to move every important file into it. You probably have dozens of files in your downloads folder, in your documents folder, or on your desktop. What if you miss one? Backup should be effortless, and endpoint protection is about safeguarding every file, not just the ones in a certain folder.

### Bottom Line

Retrospect Backup protects your business from what ifs. It's an insurance policy on your business data. You have insurance for your office, your house, your car, and your health. Your business data deserves one too.

retrospect.com/try