A Business Continuity Solution for Ransomware

ShareSync by HAZCloud, a 2-in-1 backup and file sharing service, offers a complete file management solution. Among its benefits: users stay up-and-running during a ransomware outbreak.

ShareSync

Instantly roll back to uninfected files

Immediately access those clean files on any device

Keep users productive while IT restores infected computers

Avoid paying ransom to criminals

Plus: save money with a 2-in-1 backup and file sharing service

ShareSync combines real-time backup and file sharing into a single product. This 2-in-1 feature set enables file collaboration similar to Box and Dropbox alongside complete file backup and recovery across any failure scenario, like Carbonite and Mozy.

In the event of a ransomware outbreak, this combination of features—which can only be found in a 2-in-1 file sharing and backup service—keeps infected users productive. It also takes the pressure off of IT. Instead of being pressured by users who are demanding their computers, they can take the time they need to carefully contain the virus and patch any security holes.

	ShareSync	**File Sharing** Dropbox, Box, OneDrive	**Backup** Carbonite, Mozy, CrashPlan
Web and mobile access to files	🟢	🟢	🔴
Real-time (not scheduled) backups: files are backed up every time they change	🟢	🟢	🔴
Syncs major content folders (desktop, documents + shared folders)	🟢	🔴	🟢
Point-in-time restoration from backup	🟢	🔴	🟢

HAZCLOUD

How ShareSync protects you during a ransomware attack

If any user in your business gets hit with ransomware, you should instantly close the computer and isolate it from your network. The computer needs to be wiped and restored from backup. These are the best practices that will prevent the infection from spreading. However, if you have ShareSync in place, your users won't be idled during this process. Here's how it works.

Step 1

Close or isolate the infected computer(s)

Your first priority is to ensure the crypto-ransomware doesn't spread. Close any computer that's infected. Cut off network access if you have to—whatever you have to do until you get the infection contained. Call IT support immediately.

Step 2

Roll back ShareSync's file archive

Using an uninfected computer, your IT support person will access ShareSync's admin settings and roll-back the user's folders to the moment in time just before the infection occurred.

Step 3

Get back to work using alternate devices

You can get back to work using any other PC or mobile device. On the PC, you can access files through ShareSync's web interface; on a tablet or phone, you can use the ShareSync app. Meanwhile, your IT support will work on restoring the original device. Any edits you make to files will be synced to the original device as it's being restored.

Key features of ShareSync

- **File backup.** Features include real-time (not scheduled) backup, restoration to any point in time, backup and retention policies, and more.
- **File sharing and collaboration.** Sync & share files internally and externally using virtually any device. Maintain control over file access permissions
- **Admin control and security.** Keep your data safe and protected while consolidating two separate services to lower your costs.
- **Business continuity and disaster recovery.** ShareSync keeps operations up and running across a number of scenarios, from stolen devices to ransomware outbreaks.
- **Works with any platform.** ShareSync integrates with Office 365 and many other email platforms.
- **Highly reliable.** 99.999% SLA guarantees less than 26 seconds of unplanned downtime every month.