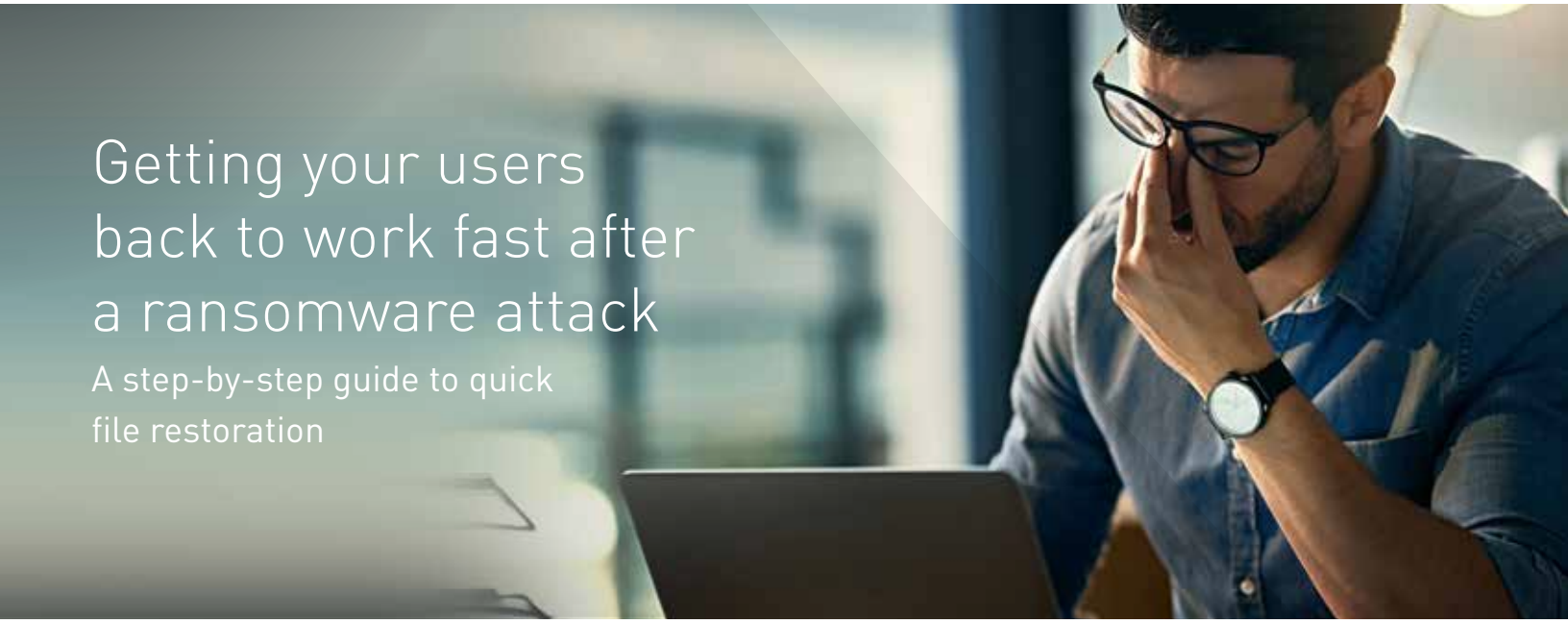
Business Solutions™
Powered by Intermedia



Getting your users back to work fast after a ransomware attack

A step-by-step guide to quick file restoration

A user's machine has been infected with crypto-ransomware. Now the files are encrypted and that user has come to you for help. This guide will show you how to quickly and easily use ShareSync's backup and file sharing solution to restore those encrypted files to their pre-infection state.

With ShareSync, users don't have to wait for you to restore their computer to get back to work. You just need to roll the files back to a clean version, and then your end users can access those files via the web on another computer or using the app on a mobile device.

There are two parts to the file restoration process:

1. figuring out what time and date to roll the files back to, and
2. performing the actual file restoration.

DETERMINE WHEN THE INFECTION HAPPENED

The time when a ransomware infection becomes apparent to the user is not necessarily the time when the infection began, so you have to track the source of the infection to find out when the malware started encrypting files. Unfortunately, this is not easy to do.

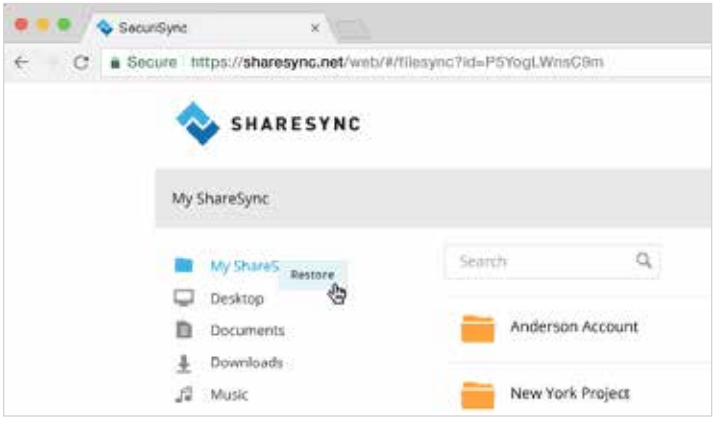
If you can't spend the time to fully investigate and find the source of the infection, you can approximate it. Here are a few ways to estimate the date and time when the files got encrypted:

1. If you believe the infection started from a phishing email, look for the date and time when that email arrived in the user's inbox.
2. If the files have new extensions, search for the encrypted file extensions and choose the earliest timestamp. In this case, the user's original files will also be found in the Deleted Items area in the backup and file sharing application, and you can use that timestamp. To find Deleted Items, select the filter in the left navigation pane.
3. If the encrypted files show no modification of extension or filename, look for groups of files that have the same modification timestamp and choose the earliest.

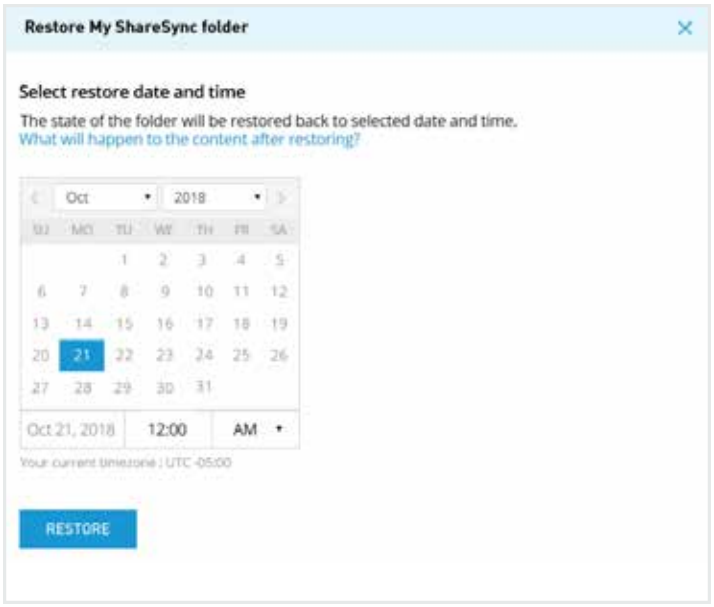
RESTORE INFECTED FILES

The advantage of ShareSync's backup and file sharing solution is that you can restore all of the encrypted files to their original state and get your users back up and running before you even reimage the infected machine. All you need is a spare laptop or tablet with internet access.

1. Log into HostPilot using your admin credentials.
2. Go to Services > ShareSync.
3. Go to Manage & Restore Files.
4. Select "Login to ShareSync as Admin".
5. Search for and select the infected user from your user list.
6. Right-click on each top level folder in the hierarchy to perform a mass restore or drill down folder by folder to perform a selective restore. (If the infected user has "modify" permissions for the folder, a restore has to be performed from the folder owner's account.)



7. Select date and time for restore. Use the estimated timestamp you found earlier, but drop it back 1 hour to give yourself a buffer.



Wait till files are restored and you're done! Now you've restored the files, and your users are ready to get back to work.

Note: You might need to adjust the selected time and perform the restore again if the estimated timestamp you chose turned out to be later than the infection, even with the extra hour.

GUIDANCE FOR THE USER

Any changes your user makes and saves to their files will be synced to their reimaged machine when you fix it and give it back. So don't worry about versioning; just make sure your user syncs their files back up to the app. For shared files, the clean version will automatically sync to the team's computers.

OTHER CONSIDERATIONS REGARDING THE INFECTED MACHINE

If you plan to use the infected hard drive again, we recommend that you perform a NIST secure wipe on it before reimaging. This ensures that the infection is completely removed. Alternatively, you can save the infected drive for law enforcement if you plan to report the incident.