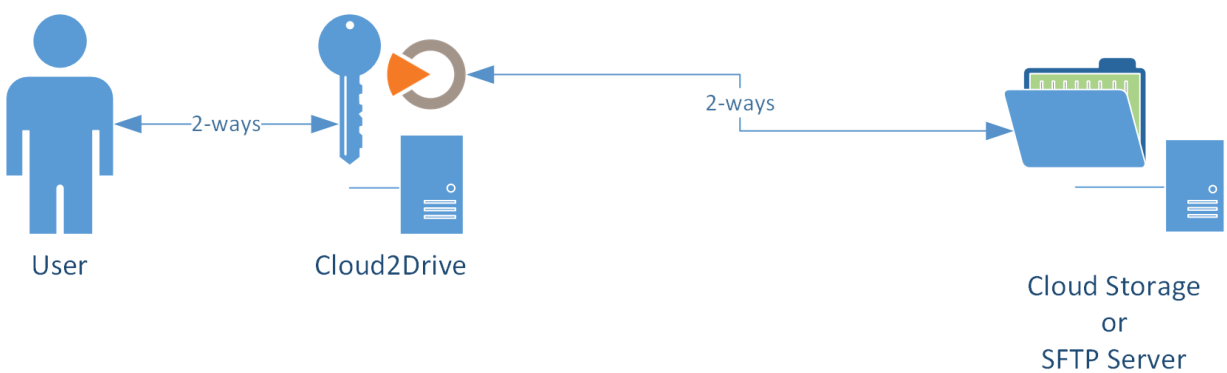
CLOUD2DRIVE-PROTECTED ONLINE STORAGE IS IMPERVIOUS TO RANSOMWARE BY USING SILVERSHIELD

Ransomware is a type of malware that restricts access to the infected computer system, and demands that the user pay a ransom to the malware operators to remove the restriction. Probably the most famous ransomware, even though not the only one, is Cryptolocker, and it's certainly something you don't want to deal with.

Regardless of the strenuous efforts put in place by Antivirus developers, the rate of infection these days is astonishing with an unprecedented outbreak of infection. To make things even worse, ransomware can also access all the shared folders on your NAS/SAN, so **if you backup to a network drive your backups will be compromised too**. This is because the ransomware goals include preventing you from being able to restore your old (healthy) data from a backup.

Now, the only way for Cloud2Drive to serve its very purpose (providing users with a secure way to access and use online, cloud and non-cloud, storage) is to allow bidirectional read and write operations:

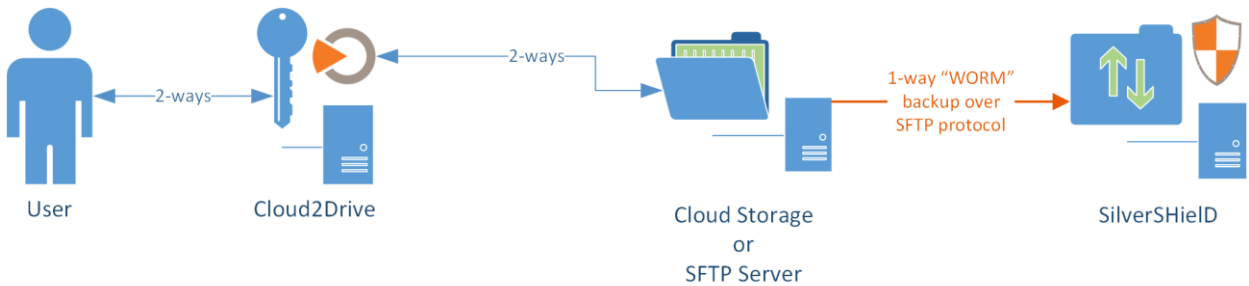


By Cloud2Drive showing, acting and behaving just like a "drive," it is theoretically possible that ransomware might access and lock down files on the remote online storage.

Fortunately, it is easy to make Cloud2Drive-protected online storage truly impervious to ransomware:

Using Extenua's SilverSHielD, administrators can create an SFTP user profile for backup purposes and then remove the *delete, rename and modify* permissions from the SilverSHielD Management Console. This ensures that, once stored, **backups cannot be altered** anymore, in any way, via the SFTP server.

Ransomware's goal is maximum efficiency, therefore no ransomware would even try to break into an SFTP server; furthermore, even if it tried, the key exchange and PKI authentication would stop it before it even gains any type of access. This ensures that backups are **incremental and inalterable**, like they would be in a true WORM ("write once read many") backup medium:



The only thing left to do now is to make sure that both of the following rules are enforced:

- The backup software running on Extenua customers' cloud/online storage must be configured to use their SFTP server as a target
- The OS user on the machine that runs the backup software does not have any other access to the machine where the backups will be stored except SFTP (remove all SMB/CIFS "shares")

And that is it. In the event of a ransomware infection, users will simply be able to format their computer, reinstall their operating system, and **restore all data from an always-healthy backup**.