You cannot read an industry publication today without seeing articles about real-world cases of ransomware. The attackers hack the network, encrypt the primary data, take control of the backup application and backup storage - and delete the backups. There is no way to recover. And, unless you pay the ransom you cannot operate your business.

Let’s assume that the primary storage is encrypted, and the hackers took control of the backup application or backup storage and issued ‘delete all’ data commands. In this case, if the backup storage is low cost primary storage disk or a deduplication appliance, then the backup data is deleted and there is no way to recover.

**HOW TO GUARD AGAINST THIS RISK?**

First, you need to have a network-facing tier of storage for high speed backups and restores. Second, you need a second non-network-facing tier for long-term retention. The hackers can get to the network-facing tier but not the tier that is not on the network (this creates an air gap).

Second, you need a policy-driven backup system that delays delete requests. If a delete request is issued, the network-facing tier is deleted, however the second non-network-facing tier driven by the policy does not process the deletes for days or weeks, depending on the policy setting. If the policy is set to 30 days then the delete request won’t execute for 30 days. When a ransomware event happens you simply go to the backup storage second tier and recover, as any backups in the second tier are not immediately deleted.

In addition, the second tier, typically a long-term retention tier, needs to have deduplication objects that are immutable; meaning they are never changed, deleted or overwritten. If any data is encrypted in or written to the first tier of storage from the backup application, the new deduplication objects are added but never overwrite the previous deduplication objects. This approach ensures that the long-term retention data is not compromised.

The combination of a primary tier for performance, coupled with a non-network-facing tier for long-term storage that has delayed deletes, ensure that the backup data is not deleted and ready for restore. The combination of a second non-network-facing tier coupled with immutable deduplication objects ensures the long-term retention data is not comprised. You can restore the primary site data and you still have all your long-term retention data.

To keep up to 30 days of delayed deletes only takes an additional 10% of storage versus a total separate retention lock store that can double the backup storage and requires maintaining two data stores. This new advanced approach is called Retention Time-Lock and is only available from ExaGrid.

More info: www.exagrid.com