



ExaGrid Retention Time-Lock for Ransomware Recovery

DATA SHEET



ExaGrid Wins Storage Awards' "Enterprise Backup Hardware Product of the Year – 2019"



ExaGrid Voted Network Computing's "Hardware Product of the Year – 2019"



ExaGrid Voted SVC's "Hyper-convergence Company of the Year – 2018"



DCIG Rates ExaGrid #1 "Recommended Deduplicating Backup Appliance" in 2018 Buyer's Guide



ExaGrid Named "Visionary" in the 2015 Magic Quadrant for Disk Backup with Deduplication Appliances

Ransomware attacks are on the rise, becoming disruptive and potentially very costly to businesses. No matter how meticulously an organization follows best practices to protect valuable data, the attackers seem to stay one step ahead. They maliciously encrypt primary data, take control of the backup application and delete the backup data.

Protection from ransomware is a primary concern for organizations today. ExaGrid offers a unique approach to ensuring that attackers cannot compromise the backup data. The software release targeted for the fall of 2020 allows organizations to be confident they can restore the affected primary storage and avoid paying ugly ransoms.

The challenge is how to protect the backup data from being deleted while at the same time allow for backup retention to be purged when retention points are hit. If you retention lock all of the data, you cannot delete the retention points and the storage costs become untenable. If you allow retention points to be deleted to save storage, you leave the system open for hackers to delete all data.

ExaGrid's unique approach is called Retention Time-Lock. It prevents the hackers from deleting the backups and allows for retention points to be purged. The result is a strong data protection and recovery solution at a very low cost of storage.

ExaGrid is Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Retention Tier containing all retention data. Data is written directly to the "network facing" ExaGrid disk-cache Landing Zone. Then it is tiered into a "non-network facing" long-term retention repository where it is stored as deduplicated data objects to reduce the storage cost of long-term retention data. As data is tiered to the Retention Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata never change allowing only for the creation of new objects or deletion of old objects when retention is reached.

ExaGrid's approach to ransomware allows organizations to set up a time lock period that governs the processing of any delete requests in the Retention Tier as that tier is not network facing and not accessible to hackers. The combination of a non-network facing tier, a delayed deletion for a period of time and objects that never change are the elements of the ExaGrid Retention Time-Lock solution. For example, if the time lock period for the Retention Tier is set to 30 days, then when delete requests are sent to the ExaGrid from a backup application that has been compromised or from a hacked CIFS or other communications protocols, the data in the Retention Tier is time-locked for up to 30 days against any deletion. The data in the Landing Zone will be deleted or encrypted, however, the Retention Tier data is not deleted upon an external request for the configured period of time. When a ransomware attack is identified, simply put the ExaGrid system into a new recover mode and then restore any and all backup data to primary storage.

The solution provides a retention lock, but only for an adjustable period of time as it delays the deletes. ExaGrid chose not to implement Retention Time-Lock forever because the cost of the storage would be unmanageable. With the ExaGrid approach, all that is needed is up to an additional 10% more repository storage to hold the delay for the deletes. ExaGrid allows the delay of deletes from 1 day to 30 days.



ExaGrid Retention Time-Lock for Ransomware Recovery

Recovery Process – 5 Easy Steps

- Invoke recover mode.
 - Retention Time-Lock clock is stopped with all deletes put on hold indefinitely until data recovery operation is complete.
- Contact assigned level 2 ExaGrid customer support engineer.
 - The backup administrator can carry out the recovery using the ExaGrid GUI, but since this is not a common operation, we suggest contacting ExaGrid customer support.
- Determine the time of the event so you can plan restore.
- Determine which backup on the ExaGrid completed deduplication before the event.
- Perform restore from that backup using the backup application.

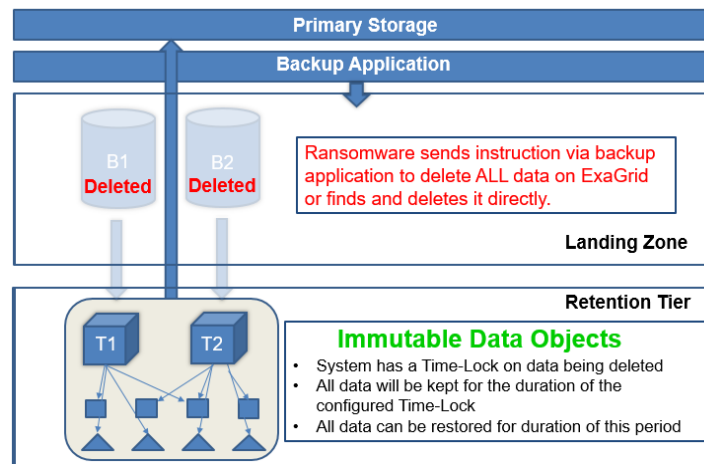
ExaGrid advantages are:

- Manage a single system instead of multiple systems for both backup storage and ransomware recovery
- Unique second Retention Tier that is only visible to ExaGrid software not to the network
- Data is not deleted as delete requests are delayed and therefore ready to recover after a ransomware attack
- Weekly, monthly, yearly and other purges still occur to keep storage costs in line with the retention periods
- Only requires up to an additional 10% of repository storage
- Storage does not grow forever and stays within the backup retention period set to keep storage costs down
- All retention data is preserved and is not deleted

Example Scenarios

- Data is deleted in the ExaGrid Disk-cache Landing Zone via the backup application or by hacking the communication protocol. Since the Retention Tier data has a delayed delete time lock, the objects are still intact and available to restore. When the ransomware event is detected, simply put the ExaGrid in a new recover mode and restore. You have as much time to detect the ransomware attack as the time lock was set for on the ExaGrid. If you had the time lock set for 14 days, then you have 14 days to detect the ransomware attack and put the ExaGrid system in the new recover mode for restoring data.

Deletion of Backup Data on ExaGrid



United States: 350 Campus Drive | Marlborough, MA 01752 | (800) 868-6985

United Kingdom: 200 Brook Drive | Green Park, Reading, Berkshire RG2 6UB | +44 (0) 1189 497 051

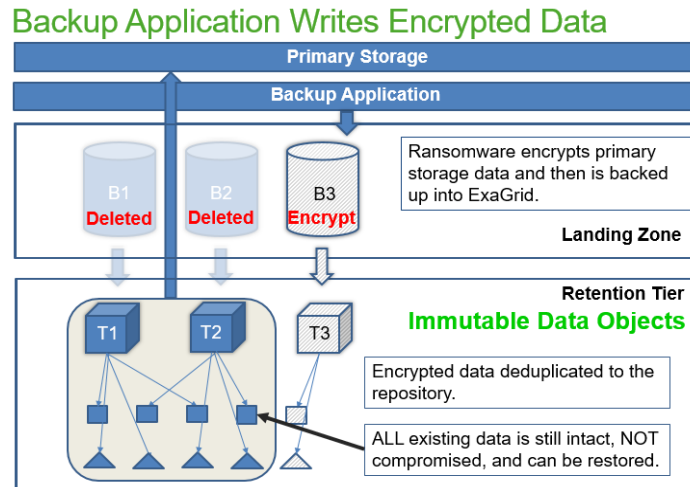
Singapore: 1 Raffles Place, #20-61 | One Raffles Place Tower 2 | 048616 | +65 6808 5574

EXAGRID[®]

www.exagrid.com

ExaGrid Retention Time-Lock for Ransomware Recovery

- Data is encrypted in the ExaGrid Disk-cache Landing Zone or is encrypted on the primary storage and backed up to ExaGrid such that ExaGrid has encrypted data in the Landing Zone and deduplicates it into the Retention Tier. The data in the Landing Zone is encrypted. However, all previously deduplicated data objects never change (immutable), so they are never impacted by the newly arrived encrypted data. ExaGrid has all previous backups before the ransomware attack that can be restored immediately. In addition to being able to recover from the most recent deduplicated backup, the system still retains all the backup data according to the retention requirements.



Features:

- Any deletion requests are delayed by the number of days in the protection policy.
- Encrypted data written to ExaGrid does not delete or change previous backups in the repository.
- Landing Zone data that is encrypted does not delete or change previous backups in the repository.
- Set delayed deletion in 1 day increments from 0 days to 30 days.
- Protects against loss of any and all retained backups including monthlies and yearlies.
- Two-Factor Authentication (2FA) protects changes to Time-Lock setting.
 - Only Administrator role is allowed to change Time-Lock setting.
 - 2FA with administrator Login/Password and system generated QR code for second factor authentication.
- Separate password for primary site versus second site ExaGrid.
- Security Officer password to change or turn off Retention Time-Lock.

United States: 350 Campus Drive | Marlborough, MA 01752 | (800) 868-6985

United Kingdom: 200 Brook Drive | Green Park, Reading, Berkshire RG2 6UB | +44 (0) 1189 497 051

Singapore: 1 Raffles Place, #20-61 | One Raffles Place Tower 2 | 048616 | +65 6808 5574

EXAGRID[®]

www.exagrid.com