Druva and immutability

The challenge

Ever since backup and archive shifted from tape to disk, customers have worried that all of their backup data could be damaged due to one of the following risks:

- **External risks:** Corruption or deletion of backups outside of the backup system administrative interface (i.e. bit rot, direct deletion or corruption/encryption by a bad actor)
- **Internal risks:** Deletion of backups via the backup system administrative interface (i.e. mistake by a system administrator, actions of a rogue administrator, or a bad actor masquerading as an administrator)

Therefore, a complete immutability solution must address both external and internal risks.

How do data protection vendors address these risks?

Most backup vendors do not have a method for addressing either of these risks. Often, backups are stored on an on-premises disk that is electronically accessible and vulnerable to direct attacks, and not protected against long-term concerns like bit rot. This is why there are many stories in the press about backup data being encrypted during a ransomware attack. There is also usually no protection against an authenticated administrator that accidentally or maliciously damages the backups.

Typical responses today to improve security include the following:

- **Multi-factor authentication** (MFA)
- **Extended recycle-bin** (delaying garbage collection)
- **Copy backups** to immutable storage in the cloud

The use of MFA should be encouraged, but should only be part of the picture. It only deters a bad actor, and does not stop one that has infiltrated your secondary authentication system. It also does not address accidents or malicious acts by a rogue administrator.

The recycle-bin approach, where deleted backups aren't actually deleted for some period of time, is also a good idea, but only addresses part of the problem. It also only works if the customer notices the deletion soon enough to repair it.

Finally, some vendors now support the ability to copy some backups into immutable storage in the cloud. Although this approach does address both concerns, it only addresses them for that copy – on premises copies are still at risk. This additional copy also increases the customer's storage costs.

None of these approaches fully protects all backups from both external and internal risks. A proper approach would address both concerns by fully protecting all backups at the storage level, as well as providing optional protection from accidental or malicious deletion via the user interface.

Only Druva's approach addresses both concerns for all backups

Druva is the first DPaaS vendor to address both risks with a multi-layered security model ensuring customer backup data remains immutable (i.e. unchanged) for their chosen retention period.

External threats

- All backups air-gapped in Druva's hardened S3 account
- External access to backup data blocked via IAM, RBA, MFA, and bastion hosts
- No SSH access to any Druva hosts
- All backup data encrypted in transit and at rest with customer-managed keys
- Metadata needed to assemble sharded data stored in separate system

- 99.999999999% durability via S3
- Regular integrity scans to address bit rot
- Anomaly detection of ransomware attack

Internal threats

- Role-based administration
- Multi-factor authentication (native and via OKTA)
- Delayed deletion of backup data (i.e. recycle bin)

Key benefits

For years, Druva has provided a level of security, immutability, and integrity not seen in any competitors. Druva is also working on additional features to keep your backups even more secure.

- **Air gap:** All backups are stored in Druva's S3 account, completely separated from the customer's computing environment. This protects them from any malware or ransomware that might infect other backup systems.
- **Integrity:** The first layer in Druva's approach is resilience. Druva stores its customers' backups on the highly resilient AWS S3 platform that provides triple redundancy, 99.999999999% durability, and regular integrity scans to detect and repair bit rot.
- **Intrusion detection and prevention:** Druva performs a variety of activities to protect from any direct attacks by bad actors directed at the backup data itself. First, backup data and metadata are encrypted and stored in the cloud on the other side of a virtual air gap, which protects it from things such as ransomware attacks that have encrypted the backups of competitors' customers. Several technologies prevent unauthorized access to or modification of this backup data, including IAM and bastion hosts, RBA, and MFA, and no SSH access to Druva's production systems.
- **Information protection:** Druva's deduplication process provides an additional level of protection by slicing all backups into chunks, encrypting each chunk in transit, and storing it as an encrypted object in S3. Backup data chunks are stored separately from the metadata required to reconstruct these chunks into their original form. These techniques prevent backups from being used as a method to steal confidential information to use in a ransomware attack.
- **Anomaly detection and deletion prevention:** Druva uses machine learning-based anomaly detection to further protect customer data. For example, Druva can automatically detect and notify customers of a possible ransomware attack. The system can also detect the excessive deletions of backups and pause said deletions until the Druva team can verify this with the customer.

Druva believes the combination of these protection features provides a level of protection unavailable with its competitors. In addition, Druva is developing even more protection features that will be available to customers in the coming months/year. Unlike Druva's competitors, these features will apply to *all copies of all backups*.

For more information

To learn more about how Druva can empower your business with unified data protection and management, visit the Druva Cloud Platform overview page.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com