

PUBLIC CLOUD SERVICES

AIR GAP RECOVER

Cloud-native, cloud scale data protection

Safeguard your cloud-native data with Air Gap Recover, and guarantee rapid recovery, with automated failover and near-zero downtime.

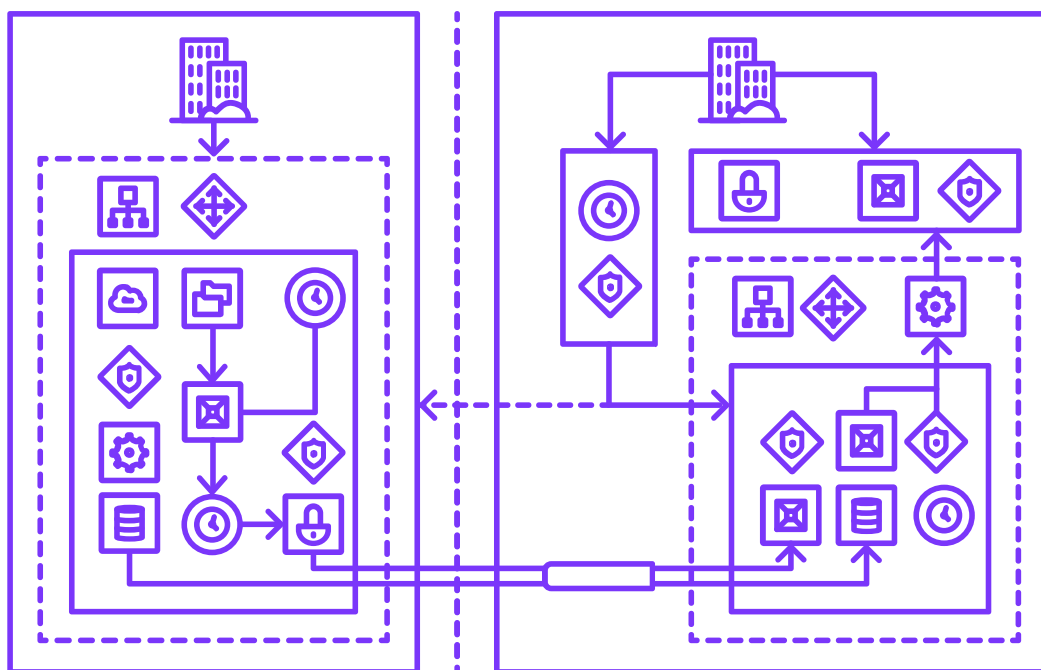
Engineered for cloud-native systems – Databarracks' Air Gap Recover delivers scalable, secure protection for petabytes of data across AWS services like S3, RDS, EFS, and FSx.

In the event of a cyber attack, it guarantees a clean and lightning-fast recovery at scale.

Traditional solutions fall short

For cloud-native organisations, securing data once meant choosing between enterprise solutions and the built-in tools provided by the cloud platforms. But these conventional options fail to meet the unique demands of cloud-native organisations.

- Enterprise solutions struggle to scale and are often slow and impractical to use.
- In-built cloud tools are too limited. Narrow in scope, the native tools lack the functionality to truly protect your data.
- Recovery is compromised. Recovery takes too long, or worse still, there is no clean copy of data to recover from at all.



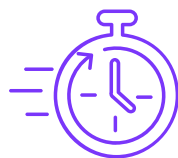
PUBLIC CLOUD SERVICES

AIR GAP RECOVER

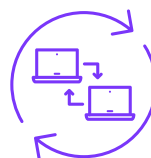
How it works



Step 1: Secure all your cloud assets. Your cloud object and block data, container file systems, database services, and code repositories are protected, ensuring no part of your environment is left vulnerable.



Step 2: Enable cross-region failover into a completely isolated, separate cloud account. Even if your primary cloud account is compromised, your failover account remains untouched, and ready to activate instantly.



Step 3: Automate your recovery via Infrastructure as Code. Using IaC, your entire cloud environment – EC2 instances, databases, and networks – is restored automatically.

Tagging and replication

S3 buckets you need to protect are tagged, and a Lambda script runs a replication job to securely copy data. Each replication is encrypted and flagged within AWS Control Tower for tracking.

Data integrity

Each replication job has its own encryption key, ensuring that re-writes are safe and secure. In addition, versioning is enabled to provide further protection against accidental overwrites or deletions.

Custom snapshots

For databases stored in RDS, custom snapshots are set up to ensure regular backups. The snapshots are then automatically copied over to a secure S3 bucket, ensuring that your critical database information is safely stored in an isolated environment.

RDS and EBS similarity

EBS (Elastic Block Store) works similarly to RDS in our protection strategy. EBS stores data for your EC2 instances, and snapshots are taken that are regularly backed up and replicated to a secure S3 bucket.

Container storage protection

EFS, commonly used for container storage, is securely backed up by replicating it to an S3 bucket. These backups are also replicated to an additional AWS account for increased resilience and redundancy.

Code repository protection

Secure replication of Git or Bitbucket repositories is implemented, ensuring that your code and version history are backed up and available for recovery. This adds an extra layer of protection to your development environments.

Comprehensive repository protection

Protection extends to the broader organisation, ensuring that repositories and organisational resources are safeguarded. This means that in the event of an issue, you can recover not just your data but also your operational processes and environments.