CONTOUR SECURE CLOUD

Recover your data. Keep your business moving.

Air-Gapped Tertiary Site Recovery combines an isolated recovery vault with enterprise IaaS. Give critical applications an alternate place to operate while your primary environment is investigated and restored.

Isolate
A separately controlled recovery copy

Validate
Test selected copies and applications

Operate
Run approved workloads in IaaS

Air-Gapped Tertiary Site Recovery / AGSR

An isolated recovery layer
Preserve selected recovery copies apart from everyday production connectivity and administration.

A validated path back
Plan how candidate recovery points and application dependencies are tested before operation.

Somewhere to operate
Prepare separate cloud compute, storage and networking for priority recovered workloads.

People and a defined process
Connect Contour expertise, documented runbooks and agreed recovery responsibilities.

Where will your business run after a breach?
A protected recovery copy needs a usable destination. AGSR connects isolation and recovery planning with Contour Cloud IaaS, sized around the applications your business needs first.

THE RECOVERY ARCHITECTURE

Isolate. Validate. Recover. Operate.

Design the recovery copy, the access controls and the operating destination together. Each part is selected around your workloads, technology and business priorities.

01 Production to landing zone

Identify the workloads and data your business needs to recover. Selected copies enter a Contour Cloud landing zone through a planned transfer path. Agree on transfer cadence, retained history, connectivity and monitoring. These choices influence the recovery points available when an incident occurs.

02 Controlled transfer and isolation

Define how selected copies move from the landing zone to the tertiary vault and how connections close between transfer windows. Document the air-gap method and access controls. A different location alone does not establish isolation; the design must specify how the recovery copy is separated and controlled.

03 Separate access and retention

Establish vault access roles and recovery approvals apart from everyday production administration. Define encryption, retention and the controls that protect recovery copies. Include immutable or write-once retention where supported by the selected platform and configuration. Agree on responsibilities for monitoring exceptions and reviewing access.

04 Recovery validation

Assess candidate recovery points with the incident response team. Test selected applications and dependencies in a separate recovery environment before approving them for operation. Validate identity, databases, networking and integrations, and document the checks and decisions in the recovery runbook.

05 IaaS for continued operation

Run approved priority workloads in a planned Contour Cloud IaaS environment. The environment operating applications remains separate from the vault. Define compute, storage, virtualization, approved user access and site connectivity around business needs. Capacity readiness and operating duration are agreed before an incident.

06 A controlled return

Plan the transition back when the primary environment is ready. Define validation, data reconciliation, connectivity changes and approval responsibilities. Test the recovery sequence and update the runbook as applications change. Recovery objectives depend on the tested design and become commitments only when expressly included in the service order.

ILLUSTRATIVE USE CASE / FOOD MANUFACTURING

13 global sites. Another recovery path.

Two active-active data centers support the business. Contour adds an isolated tertiary recovery layer and a separate cloud environment for selected recovered applications.

The environment

A global food manufacturer operates across 13 sites with two active-active data centers. Illustrative priorities include identity services, ERP, inventory and warehouse systems, and order processing. Dependencies and site access shape the recovery order.

The challenge

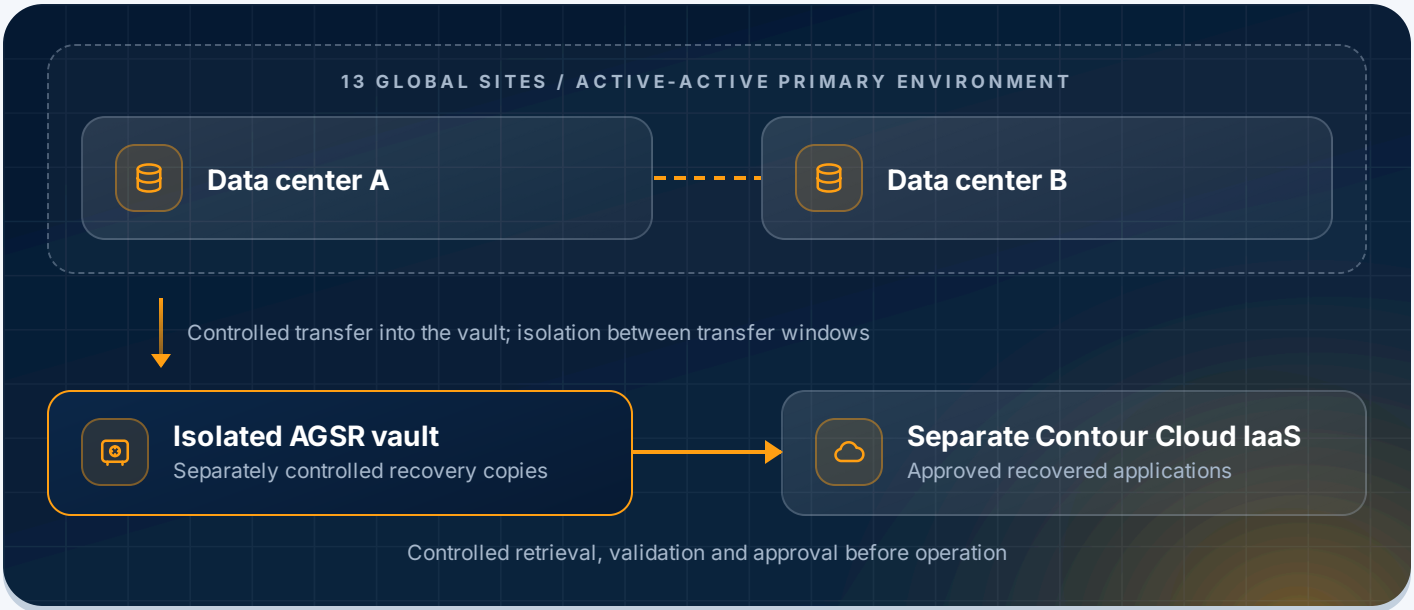
A breach could affect both data centers or shared administration. The team needs separately controlled recovery copies and an alternate operating environment while affected systems are investigated and rebuilt. Active-active availability and cyber recovery address different failure scenarios.

The Contour approach

Move selected copies through a controlled transfer workflow into the isolated tertiary vault. Assess candidate recovery points, validate applications and dependencies, then run approved priority workloads in separate Contour Cloud IaaS. Reconnect sites through planned access.

The business value

Plan how essential business systems resume operation while remediation continues. Cinch provides visibility into cloud resources and workloads through the functions available to the team. Document the return to primary systems when they are ready.



Illustrative scenario, not a named customer case study or a statement of achieved results. Workload priorities, capacity, connectivity and recovery objectives are defined during solution design.

THE CONTOUR SERVICE

Build the plan before you need it.

Work with Contour to define the tertiary site, recovery process and infrastructure required to resume critical operations. Make responsibilities clear from the start.

01 **Discover and design**
Define workload priorities, dependencies, retention and recovery objectives.

02 **Deploy and isolate**
Configure the landing zone, controlled transfer, vault access and IaaS design.

03 **Test and document**
Validate selected workloads and document recovery, escalation and return procedures.

04 **Monitor and improve**
Review agreed service components, exceptions, runbooks and changes to the environment.

Start the recovery conversation

- Which applications must return first, and what do they depend on?
- How should the vault transfer, disconnect and control access?
- What recovery points, retention and validation checks do you need?
- What IaaS capacity, operating duration and connectivity must be planned?
- Who approves recovery, security review and return to the primary environment?

Technology selected for workload fit

Protection and recovery options include Rubrik, Veeam and Zerto. Recovery IaaS may use VMware or XCP-ng, Dell PowerEdge or Cisco UCS compute, Dell, HPE or TrueNAS storage, and Arista networking. These are design options, not a universally compatible bundle. Compatibility, licensing, transfer cadence, capacity readiness, operating duration and recovery objectives are defined for your service.

Bring your critical applications. We will help map your recovery path.

Talk to an Expert ↗

484-679-2324 sales@contourds.com