dreeze

SOLUTION BRIEF

BACK MEANS BACK.

Cloud-native backup and recovery that revives complex applications to get you back to business as usual after a cyber-attack, rogue AI agent, or cloud account compromise.

THE RECOVERY SCRAMBLE

A backup restore can work as intended and yet your application isn't truly back online. Your data comes back, but the infrastructure, secrets, and connections your application needs may not.

So your team rebuilds the rest from memory: hunting credentials, digging through old runbooks, calling the one person who remembers how it all fits.

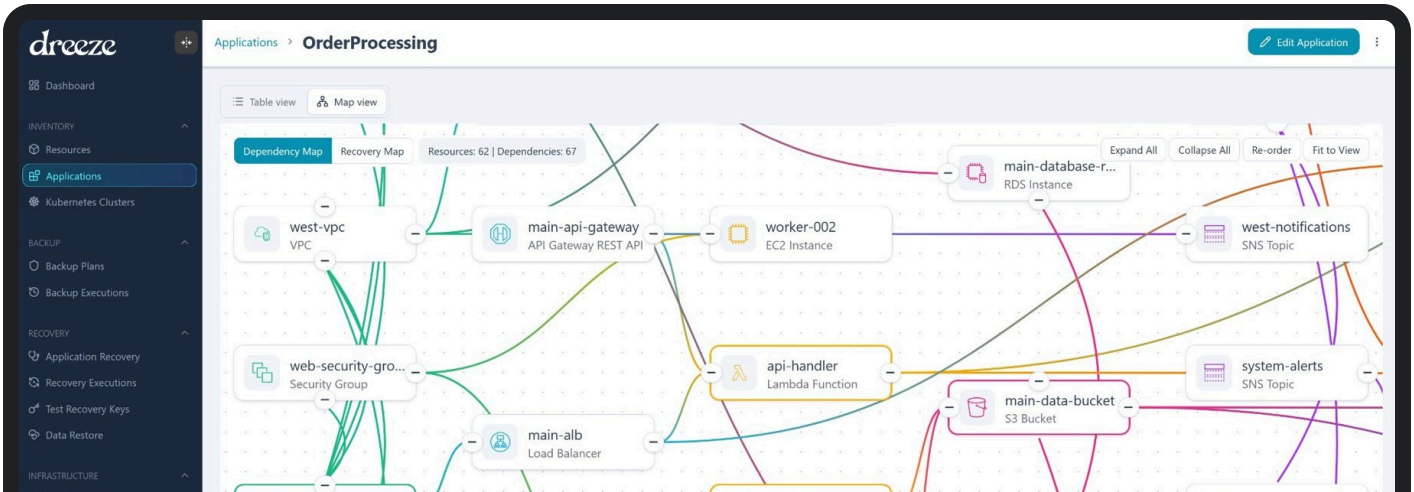
That is the recovery scramble. Hours become days while the data sits there, restored, while the application stays dead.

Dreeze goes beyond traditional backup and recovery to bring the whole cloud-native app back, not only the data.

We call it Application Revival.

KEY HIGHLIGHTS

- Every app mapped automatically from your live environment, with no tagging required
- A revival plan that rebuilds the whole app and everything it depends on, in order
- Revive apps in a clean, isolated account
- 100% SaaS for AWS and Azure, SOC 2 Type II certified, with data secure in your tenant
- API-first and MCP-ready, built to work with your automation and AI tools



HOW IT WORKS

1. KNOW

AUTONOMOUS DEPENDENCY MAPPING

Map every resource and dependency to the application it serves. Built dynamically from your live environment as it evolves, not as it looked on paper.

2. PROTECT

VAULTED BACKUP

Back up everything the application needs, from databases and volumes to VPCs, Key Vault secrets, and IAM roles. Store it all in an immutable, air-gapped vault, with optional replication across regions.

3. ORCHESTRATE

WHOLE-APP RECOVERY

Execute end-to-end recovery plan. Rebuild data, infrastructure, config, identity, and connections in dependency order without manual reassembly.

4. VALIDATE

PROVE RECOVERABILITY

Automatically run the whole plan as a non-disruptive test that doesn't impact production or require manual cleanup afterward. Every test leaves an audit-ready report.

WHERE DREEZE MAKES A DIFFERENCE

Cyber resilience	An attacker takes over a cloud account or wipes production, including KMS keys. Immutable recovery points and dependency-ordered execution bring the whole application back, not just its data, into a clean account where your security tools can check it before it goes live.
Recovery testing	Prove recoverability within your SLAs with non-disruptive tests against production data in an isolated environment, and hand auditors the report.
App downtime	A departing employee, a bad template, or an AI agent breaks the app. Recover the entire app and its full dependency chain, from the load balancer to the vector database behind its AI features.

THINGS WILL BREAK, BUT YOUR BUSINESS DOESN'T HAVE TO.

Contact us for a custom demo or a free, read-only discovery scan of your cloud environment and see your actual coverage gaps.

dreeze.com →

