

Disaster Recovery

Disaster recovery you have measured, not just written down

Recovery plans that bring servers back at another site in order, with health checks, and drills that measure the real recovery time.



TotalHeal
DisasterRecover

Contents

1 Executive summary

2 The challenge

3 Architecture

4 How it works

5 Capabilities in detail

6 Security and data handling

7 Where it fits

8 Deployment and system requirements

9 Technical specifications

10 Getting started

1 Executive summary

DisasterRecover turns the DR plan into an enforced runbook: servers recover in order at the DR site, health checks prove they work, people confirm each gate, and scheduled drills measure the recovery time and data age you would really get.

2 The challenge

Most disaster-recovery plans are documents. Nobody knows the real recovery time until the day it is needed, and on that day steps get skipped under pressure.

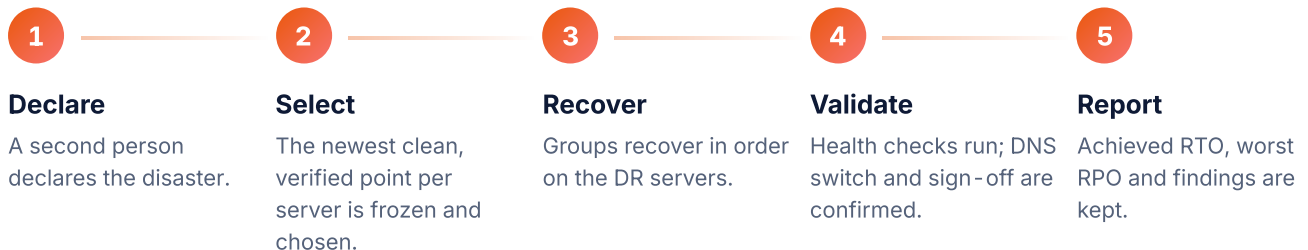
The TotalHeal approach. DisasterRecover turns the plan into a runbook the system enforces: servers recover in order at the DR site, health checks prove they work, people confirm the gates, and quarterly drills measure the recovery time you would really get.

3 Architecture



Runs restore the selected points onto DR servers in order; every gate waits for a person; reports record the achieved RTO and RPO.

4 How it works



5 Capabilities in detail

- Plans in order**
Recovery groups in order; each server mapped to the DR server it recovers on, original paths or a folder, and health checks (HTTP status, TCP connect, path exists).
- Targets and readiness**
RPO and RTO targets, worst restore-point age against the RPO, DR servers not seen for an hour, last drill and when the next is due.
- Failover runbook**
A second person declares the disaster; points are frozen; the newest clean, verified point is selected; groups recover in order; health checks run; DNS switch and business sign-off are confirmed steps; a report closes it.
- Non-disruptive drills**
Every group restores into a scratch folder on the DR server, is cleaned up and reported — every 90 days by default, started by the schedule.



Measured, not assumed

Achieved RTO, worst RPO, targets met, files and bytes restored, checks passed and failed, and findings, kept for audit.



No skipped gates

A run never skips a gate; a failed step fails the run with its reason.

6 Security and data handling

No skipped gates

Runs never skip a gate; failures stop with a reason.

Drills do not disrupt

Drills restore into scratch folders and clean up.

Two people declare

The starter cannot declare a disaster alone.

7 Where it fits

Regulator drills

Quarterly drills with measured RTO and RPO on file.

Site loss

Bring critical servers back in the right order.

Plan hygiene

See stale points and silent DR servers before the day.

8 Deployment and system requirements



Cloud (SaaS)

Available

Single-region service.



On-premises

Available

Delivered with our team from the on-premises kit.



Air-gapped

Available

Offline kit, offline licence file and offline update bundles.

Protected platforms



Ubuntu
20.04, 22.04,
24.04



Debian
11, 12



**Red Hat
Enterprise
Linux**
8, 9



**Rocky
Linux**
8, 9



AlmaLinux
8, 9

On-premises server

Operating system

RHEL, Rocky Linux or AlmaLinux 8 / 9; Ubuntu 20.04, 22.04 or 24.04; Debian 11 / 12

Processor

4 vCPU (tested configuration)

Memory

8 GB recommended (6 GB minimum)

Disk

10 GB free for software, releases and backups, plus data

Sign-in

Active Directory / LDAP, SAML 2.0 or OpenID Connect

Software

Nothing to pre-install: no container runtime, database, web

Network and access

- TotalHeal RecoveryVault
- A server at the recovery site with the TotalHeal agent

Alerts and tickets to

splunk> **Splunk**

Microsoft Sentinel

Elastic

Syslog / CEF

Jira

ServiceNow

Slack

Microsoft Teams



9 Technical specifications

Features		Included
Plans in order	✓	Included
Targets and readiness	✓	Included
Failover runbook	✓	Included
Non-disruptive drills	✓	Included
Measured, not assumed	✓	Included
No skipped gates	✓	Included
Availability by edition		Business Enterprise
Plans, readiness, failover runbook, drills, reports	✓	Included
Platforms and coverage		
Linux servers	Protected by TotalHeal RecoveryVault, with the TotalHeal agent at the DR site	
Deployment options		
SaaS (India region)	Available	Single-region service.
On-premises control plane	Available	Delivered with our team from the on-premises kit.
Air-gapped	Available	Offline kit, offline licence file and offline update bundles.
Licensing		
Priced per	Protected server per year	
Counted	Servers in a DR plan	
Trial	30 days	
Editions	DisasterRecover is sold on its own and needs RecoveryVault.	
Government profile	Government is a profile, not a separate tier or price list: the Enterprise tier with Government defaults switched on — data residency in India, four-eyes approval of policy changes, a distinct approver for every approval-level action, retention of at least 180 days, and the CERT-In and DPDP reporting clocks.	
Procurement dossier	Compliance matrix, bill of materials, architecture and hardening, SLA and OEM authorisation letter, on request	
On-premises server		

Operating system	RHEL, Rocky Linux or AlmaLinux 8 / 9; Ubuntu 20.04, 22.04 or 24.04; Debian 11 / 12
Processor	4 vCPU (tested configuration)
Memory	8 GB recommended (6 GB minimum)
Disk	10 GB free for software, releases and backups, plus data
Sign-in	Active Directory / LDAP, SAML 2.0 or OpenID Connect
Software	Nothing to pre-install: no container runtime, database, web server or Java
Requirements	
Requirement 1	TotalHeal RecoveryVault
Requirement 2	A server at the recovery site with the TotalHeal agent

10

Getting started

- TotalHeal RecoveryVault
- A server at the recovery site with the TotalHeal agent

Start a 30 days trial in the TotalHeal console with a Sttiz account. For a quote, an on-premises installation or the procurement dossier (compliance matrix, bill of materials, architecture and hardening, SLA, OEM authorisation letter), write to business@totalhealsecurity.com.

About TotalHeal

TotalHeal is a security platform from Freaquer Corporation Pvt Ltd: endpoint, network, application, cloud, security-operations and backup products, each sold on its own and run from one console.

Datasheet

totalhealsecurity.com/datasheet/disaster-recovery

No third-party certification is claimed. Figures are from our own tests where stated, with their dates. Specifications can change; this whitepaper is dated 27 October 2026.