

Cyber Recovery

Finding the newest clean restore point, and recovering with two people

After ransomware: find the newest clean restore point and roll the server back, with a second person approving.



TotalHeal
CyberRecover

Contents

1	Executive summary	6	Security and data handling
2	The challenge	7	Where it fits
3	Architecture	8	Deployment and system requirements
4	How it works	9	Technical specifications
5	Capabilities in detail	10	Getting started

1 Executive summary

CyberRecover turns ransomware alerts into a recovery incident, holds the last known-good restore point, checks restore points by bisection for the attacker's files and rolls the server back with a second person approving — moving the attacker's files aside, never deleting them.

2 The challenge

After ransomware the hard question is not whether a backup exists but which one is clean. Restore too new and the attacker's files come back; restore too old and days of work are lost.

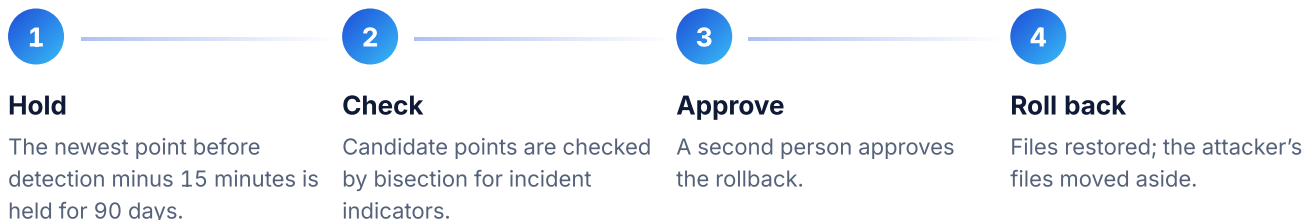
The TotalHeal approach. CyberRecover turns ransomware alerts into a recovery incident, holds the last known-good restore point, checks restore points for the attacker's files and rolls the server back with a second person approving.

3 Architecture



XDR alerts open the recovery incident; clean checks and rollbacks run as approved jobs on the server; attacker files are moved aside, never deleted.

4 How it works



5 Capabilities in detail

- Alert to recovery**
 Ransomware, inhibit-recovery and destruction alerts on a protected server open a recovery incident: the newest committed point before detection minus 15 minutes is held for 90 days and later points are marked suspect.
- Clean check by bisection**
 Up to 30 candidate points are checked by bisection: a file whose hash is an incident indicator makes a point dirty; ransom notes and encrypted copies mark it for review.
- False positives never delay recovery**
 Name-based hints only mark a point for review; they never push recovery further back.
- One-step rollback**
 Roll the server back to the chosen point with a second person approving; files the attacker created are moved aside, never deleted.



Frozen evidence

Changed files are frozen in new backups so evidence survives the clean-up.

6 Security and data handling

Never deletes

Attacker files are moved aside for evidence.

No false delays

Name-based hints never push recovery back.

Two people

Rollbacks need a second person.

7 Where it fits

Ransomware recovery

Back to the newest clean point, quickly.

Dropper hunting

Find the point before the dropper arrived.

Evidence

Changed files frozen for investigation.

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 server or Java

Network and access

- TotalHeal RecoveryVault on the servers to recover

Alerts and tickets to

splunk>

Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams



9 Technical specifications

Features		Included
Alert to recovery	✓ Included	
Clean check by bisection	✓ Included	
False positives never delay recovery	✓ Included	
One-step rollback	✓ Included	
Frozen evidence	✓ Included	
Availability by edition		BusinessEnterprise
Recovery incidents, holds, clean check, four-eyes rollback	✓ Included	✓ Included
Platforms and coverage		
Linux servers	Protected by TotalHeal RecoveryVault	
Alerts	TotalHeal XDR alerts on the protected server	
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 with CyberRecover switched on	
Trial	30 days	
Editions	CyberRecover 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 on the servers to recover

10 Getting started

- TotalHeal RecoveryVault on the servers to recover

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/cyber-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.