

Backup & Cyber Recovery

Backups that ransomware cannot read, swap or quietly poison

Encrypted, incremental backup of Linux servers and their databases, with verified restore points and ransomware detection in every backup.



TotalHeal
RecoveryVault

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

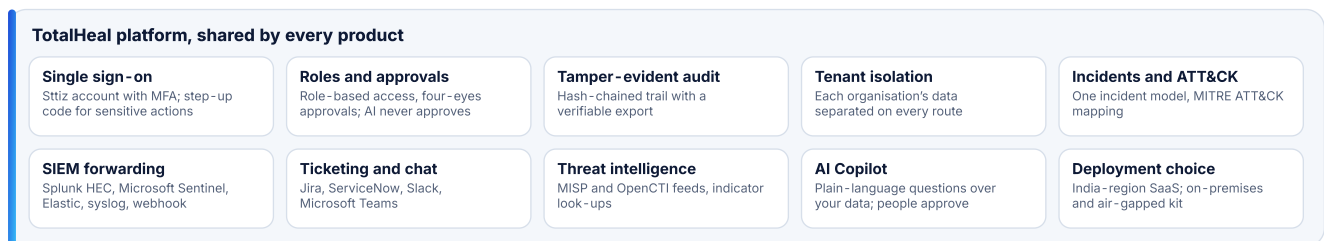
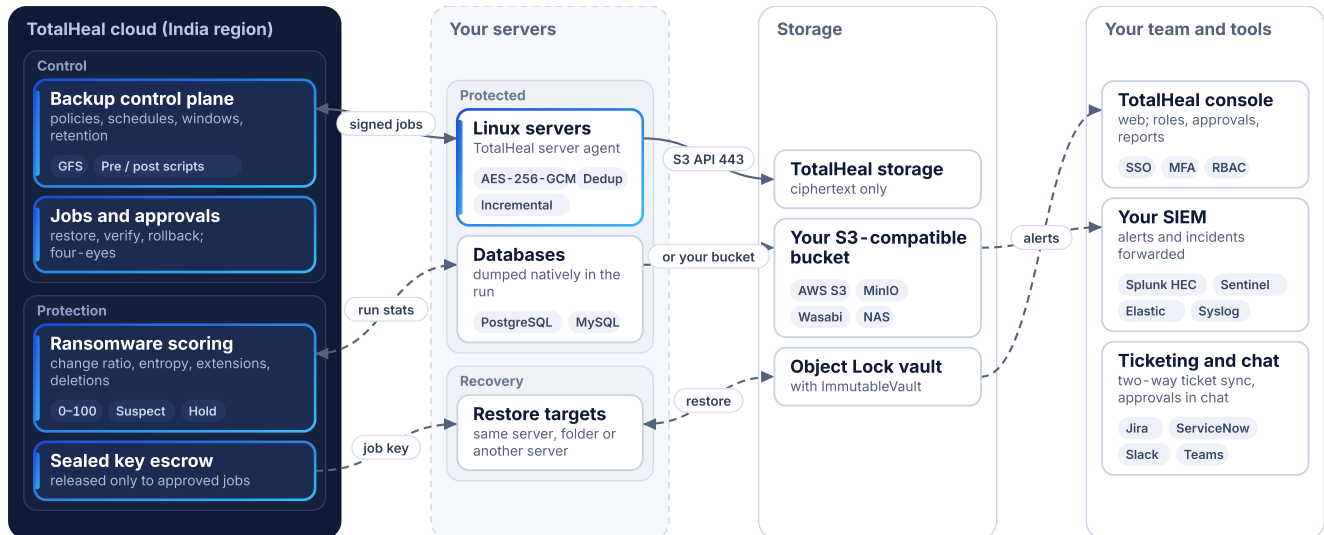
RecoveryVault treats the backup as the target it now is. Data is encrypted on the server before it leaves, every restore point is scored for ransomware as it is taken, and nothing is restored to another place without a second person. The result is a restore point you can trust on the worst day, not only a copy of the files.

2 The challenge

Ransomware now goes after backups first: it deletes them, encrypts them or waits until the bad files are in every copy. Many organisations find out during the incident that their last good backup is weeks old, unreadable or reachable with the same stolen administrator password.

The TotalHeal approach. RecoveryVault encrypts on the server before anything leaves it, keeps incremental, deduplicated restore points on your storage or ours, scores every backup for ransomware, and restores only through approved, audited jobs.

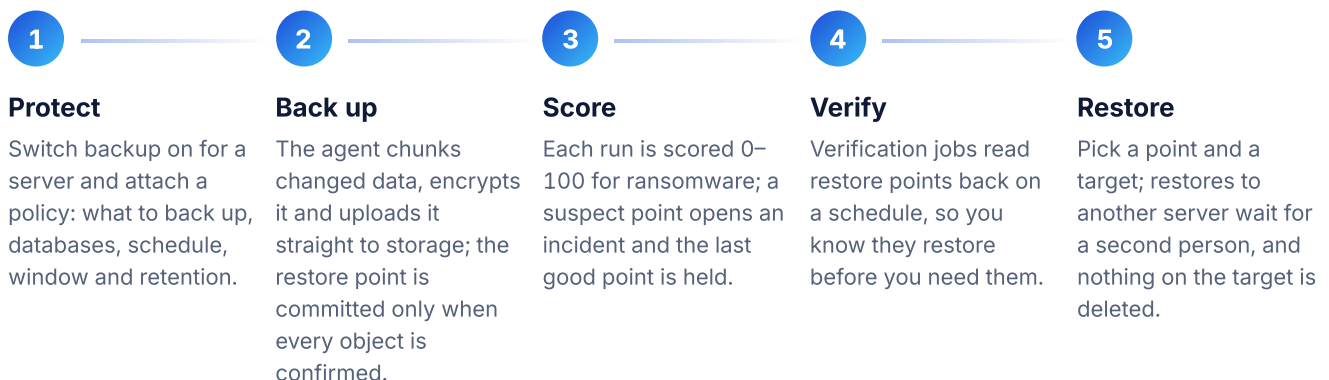
3 Architecture



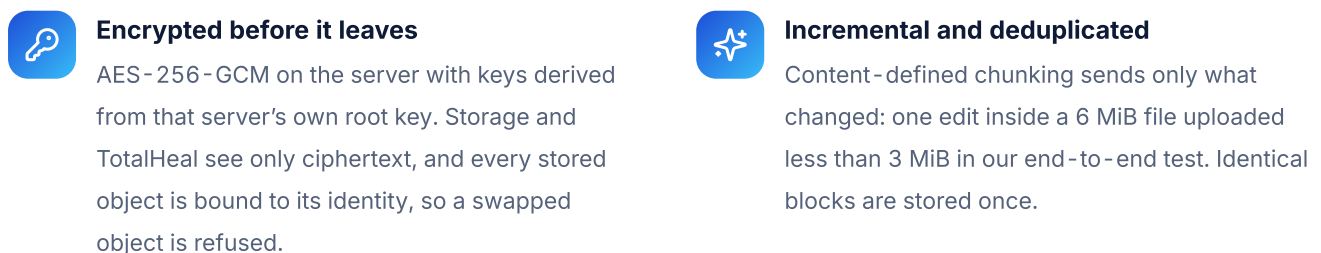
TotalHeal component
Your environment
TotalHeal cloud or edge
Third party
→ Data
 - - - → Control, optional or on approval

Backup data flows from your servers straight to storage, encrypted on the server; the TotalHeal cloud coordinates, scores, holds keys sealed and audits.

4 How it works



5 Capabilities in detail





Databases, natively

PostgreSQL and MySQL dumped by their own tools inside the backup run, with pre- and post-backup scripts for anything else that must be quiesced.



Your storage or ours

TotalHeal storage, or your own S3-compatible bucket (AWS S3, MinIO, Wasabi or a NAS with an S3 interface). Backup data goes straight from the server to storage.



Restores that never destroy data

Restore to the same server, a folder or another server. Files are written through temporary copies, verified against their checksum, and replaced files are moved aside, never deleted.



Verification

Scheduled and on-demand verification jobs read restore points back and check them, so a backup is known to be restorable before it is needed.



Schedules, windows and retention

Per-policy schedules and backup windows, and grandfather-father-son retention: daily, weekly, monthly and yearly points kept as long as you set.



Ransomware score on every backup

Change ratio, entropy jumps on normally compressible files, new extensions and deletions give a 0-100 score. At your threshold the point is marked suspect, an incident opens and the last good point is held.



Four-eyes recovery

Restores to another server and rollbacks wait for a second person; the requester can never approve their own job. Every key release and job is in the tamper-evident audit.



A lost server can be rebuilt

Each server's root key is escrowed sealed, and released only to the same server or to the agent running an approved restore job, sealed to that job's one-time key.

6 Security and data handling

Only ciphertext leaves the server

Storage and TotalHeal never see backup content; objects are bound to their identity, so a swapped object is detected.

Restores never destroy data

Replaced files are moved aside, never deleted, and every restored file is checked against its checksum.

Never held hostage

Without a licence, a server that has data stays restore-only: you can always get your data back.

Keys are released only to approved work

A server's key goes back to that server, or to the agent running an approved restore job, sealed to that job and audited.

A person, not a script, approves

Cross-server restores and rollbacks need a second person; AI never approves.

7 Where it fits

Ransomware-ready backups for Linux estates

Application and database servers backed up with a score on every run, so the incident team knows which point is clean.

Backups to your own storage

Keep data in your own S3-compatible bucket or NAS while TotalHeal runs schedules, verification and audit.

Rebuild a lost server elsewhere

Restore a failed server onto a new one with a second person approving, without anyone handling raw keys.

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

With storage inside your network.

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



PostgreSQL



MySQL

Works with



AWS S3



MinIO



Wasabi

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

- The TotalHeal server agent on each Linux server, with backup switched on
- Storage: TotalHeal's, or an S3-compatible bucket you own
- Outbound HTTPS from each server to the TotalHeal cloud and to the storage

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included	
Encrypted before it leaves	✓ Included	
Incremental and deduplicated	✓ Included	
Databases, natively	✓ Included	
Schedules, windows and retention	✓ Included	
Your storage or ours	✓ Included	
Ransomware score on every backup	✓ Included	

Restores that never destroy data	✔ Included	
Four-eyes recovery	✔ Included	
Verification	✔ Included	
A lost server can be rebuilt	✔ Included	
Availability by edition		
	Business	Enterprise
Encrypted incremental backup, databases, schedules, retention, ransomware score, restores, four-eyes approval, verification, audit	✔ Included	✔ Included
Immutable copies (ImmutableVault), clean recovery (CyberRecover), DR plans and drills (DisasterRecover)	Separate products	Separate products
Platforms and coverage		
Linux servers: Debian, Ubuntu, RHEL, AlmaLinux, Rocky	TotalHeal server agent (signed .deb and .rpm packages)	
Databases	PostgreSQL and MySQL, dumped natively	
Storage	TotalHeal storage, or any S3-compatible bucket: AWS S3, MinIO, Wasabi, S3-capable NAS	
Console	TotalHeal web console	
Deployment options		
SaaS control plane (India region) with TotalHeal storage	✔ Available Single-region service.	
SaaS control plane with your own S3 storage	✔ Available Backup data goes from your servers straight to your bucket.	
On-premises control plane	✔ Available Delivered with our team from the on-premises kit.	
Air-gapped	✔ Available With storage inside your network.	
Licensing		
Priced per	Protected terabyte per year	
Counted	Data selected for backup, in terabytes; the counting rule is set in the quote until list prices are published	
Trial	30 days	
Editions	RecoveryVault is sold on its own, outside the editions; there is no Business/Enterprise split.	

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	The TotalHeal server agent on each Linux server, with backup switched on
Requirement 2	Storage: TotalHeal's, or an S3-compatible bucket you own
Requirement 3	Outbound HTTPS from each server to the TotalHeal cloud and to the storage

10 Getting started

- The TotalHeal server agent on each Linux server, with backup switched on
- Storage: TotalHeal's, or an S3-compatible bucket you own
- Outbound HTTPS from each server to the TotalHeal cloud and to the storage

Start a 30 days trial in the TotalHeal console with a Sttizi 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/backup

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.