

Privileged Access Management (PAM)

Administrator access without anyone holding the administrator password

Vault admin passwords, broker sessions without revealing them, record everything and rotate afterwards.



TotalHeal
PrivilegeVault

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

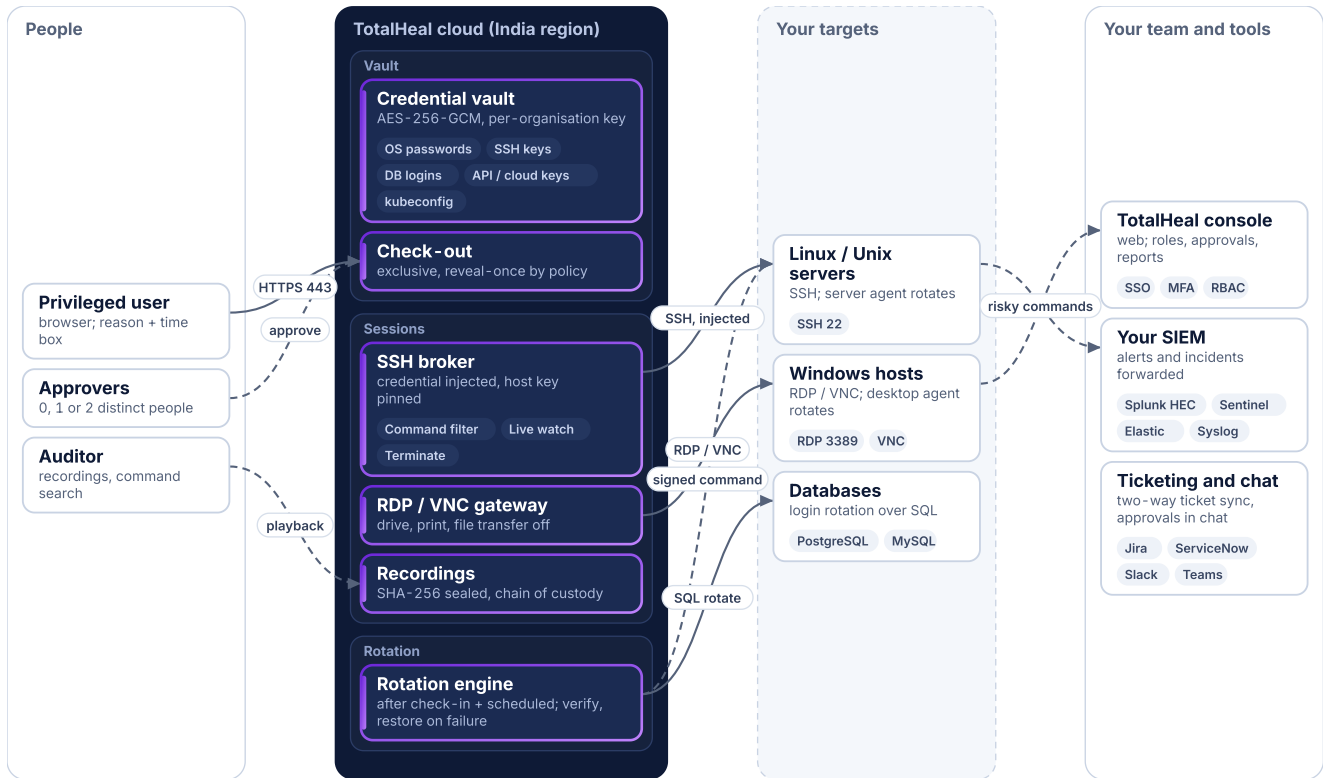
PrivilegeVault vaults privileged credentials, brokers SSH, RDP and VNC sessions without revealing them, records everything and rotates the password afterwards. Check-out needs a reason, a time box and human approval, and AI agents can never request, approve or open a session.

2 The challenge

Shared administrator passwords for servers, Windows machines and databases are known to too many people, never change and leave no record of what was done with them. One leaked admin password is often the whole breach.

The TotalHeal approach. A per -organisation encrypted vault, check-out with human approval, SSH/RDP/VNC sessions brokered without showing the password, recordings and automatic rotation.

3 Architecture



TotalHeal platform, shared by every product

Single sign-on

Sttitz account with MFA; step-up code for sensitive actions

Roles and approvals

Role-based access, four-eyes approvals; AI never approves

Tamper-evident audit

Hash-chained trail with a verifiable export

Tenant isolation

Each organisation's data separated on every route

Incidents and ATT&CK

One incident model, MITRE ATT&CK mapping

SIEM forwarding

Splunk HEC, Microsoft Sentinel, Elastic, syslog, webhook

Ticketing and chat

Jira, ServiceNow, Slack, Microsoft Teams

Threat intelligence

MISP and OpenCTI feeds, indicator look-ups

AI Copilot

Plain-language questions over your data; people approve

Deployment choice

India-region SaaS; on-premises and air-gapped kit

Users reach targets only through the broker; the credential is injected, never shown, recorded and rotated after use.

4 How it works

1

Request

A user asks for an account with a reason and a time box.

2

Approve

0, 1 or 2 distinct human approvers; never the requester.

3

Connect

The session opens with the credential injected and the host key pinned.

4

Record

Screens and SSH commands are recorded; risky commands are blocked or alerted.

5

Rotate

At check-in the password or key is rotated, verified and restored on failure.



Encrypted credential vault

AES-256-GCM with a per-organisation key; each secret version is bound to its organisation, account and version. OS passwords, SSH keys, database logins, API and cloud keys, kubeconfig. Lists never return secrets.



Sessions without the password

SSH with the credential injected and the host key pinned; RDP and VNC through a broker with drive, printing and file transfer off.



Command capture and filtering

Every SSH command recorded and searchable; deny/allow lists that block or alert; risky commands raise SOC alerts mapped to ATT&CK.



Automatic rotation

After check-in and on a schedule: Linux passwords and SSH keys, Windows local accounts on corporate devices, and PostgreSQL and MySQL logins with verify and restore on failure.



Tamper-evident audit

Every PAM action in the hash-chained audit with a verified export; risky-command alerts can be forwarded to your SIEM.



Check-out with dual control

A reason, a time box and 0, 1 or 2 distinct human approvers — the requester can never approve. Exclusive check-out and reveal-once by policy.



Recording and playback

SSH and RDP/VNC recordings sealed with SHA-256 at close, registered as evidence with chain of custody, played in the browser.



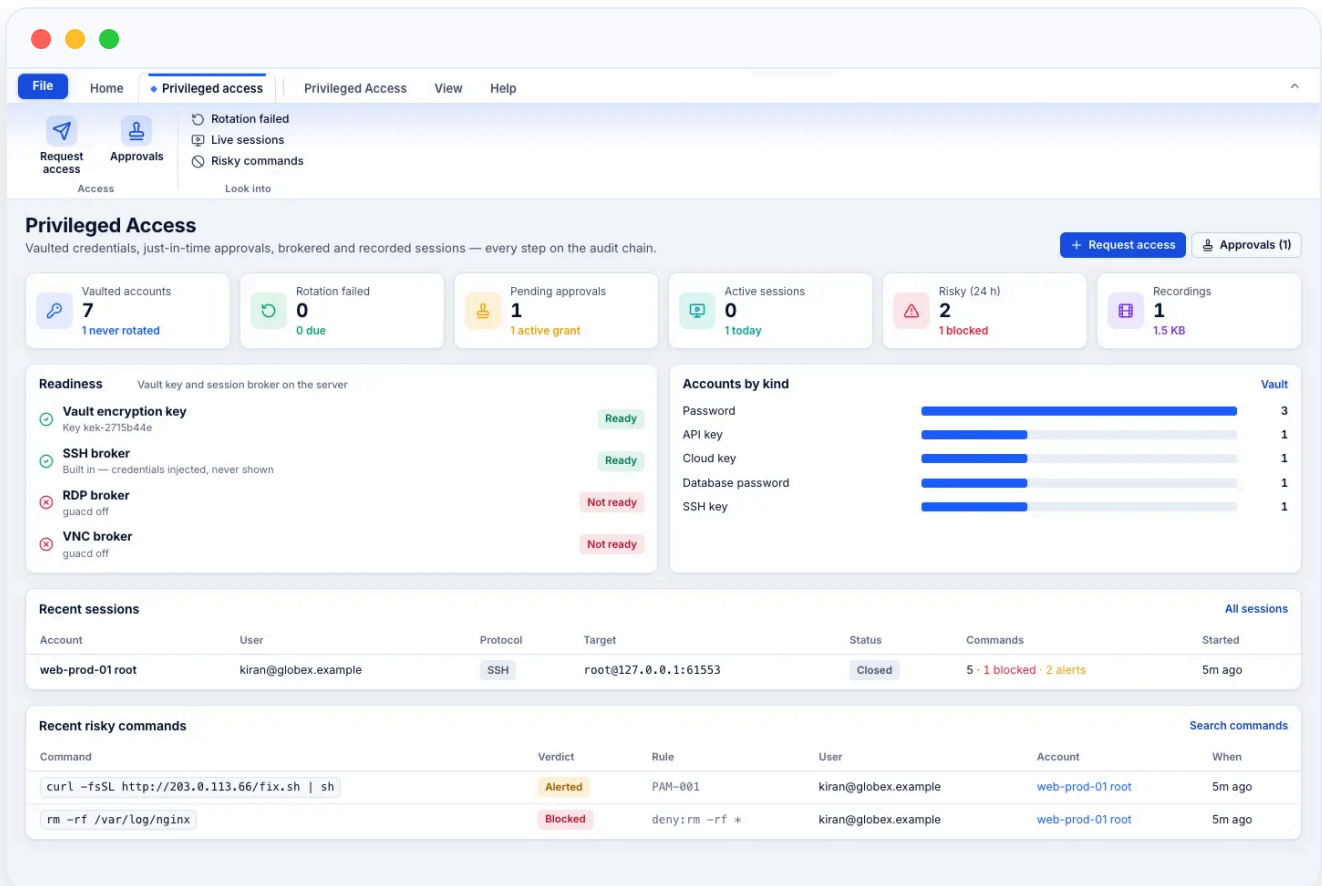
Live monitoring

Watch a running session and terminate it with a reason; idle timeout and automatic end at the time box, check-in or revoke.



Humans only

AI agents and machine identities can never request, approve, reveal, rotate or open a session.



The Privileged Access overview in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

Secrets never listed

Each secret is encrypted and bound to its organisation, account and version; lists never return secrets.

Humans only

AI agents and machine identities can never request, approve, reveal, rotate or open a session.

Sealed evidence

Recordings are sealed with SHA-256 at close and kept with chain of custody.

7 Where it fits

Shared admin accounts

Root and local administrator passwords that nobody knows and that change after every use.

Vendor maintenance

Approved, time-boxed, watched sessions for outside engineers.

Database administration

Database logins rotated automatically with verify and restore.

8 Deployment and system requirements



Cloud (SaaS)

Available

Public targets must be in your allowed networks.



Hybrid

Partial

Through a Secure Access connector node on your network (a binary today); a dedicated on-site gateway is on the roadmap.



On-premises

Available

On-premises or fully offline, delivered with our team from one kit.



Air-gapped

Available

On-premises or fully offline, delivered with our team from one kit.

Protected platforms



Linux / Unix
SSH



Windows
RDP



VNC
servers



PostgreSQL



MySQL

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

- A modern browser
- Network reachability from the broker, or a Secure Access connector
- TotalHeal server agent on Linux targets and desktop agent on Windows targets for rotation
- A database login that can change its own password for database rotation

Alerts and tickets to



Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included
Encrypted credential vault	✓ Included
Check-out with dual control	✓ Included
Sessions without the password	✓ Included
Recording and playback	✓ Included

Command capture and filtering	✔ Included		
Live monitoring	✔ Included		
Automatic rotation	✔ Included		
Humans only	✔ Included		
Tamper-evident audit	✔ Included		
Availability by tier	Essential	Professional	Elite
Encrypted credential vault (AES-256-GCM, per-organisation key) for OS, SSH and database accounts	✔ Included	✔ Included	✔ Included
Check-out with dual control: reason, time box, up to two approvers (never the requester), reveal once, check-in	✔ Included	✔ Included	✔ Included
Automatic rotation after check-in and on a schedule; tamper-evident audit	✔ Included	✔ Included	✔ Included
Sessions without the password: SSH with the credential injected, RDP and VNC through the broker, command filtering	—	✔ Included	✔ Included
Live monitoring: watch a running session and terminate it	—	✔ Included	✔ Included
Recording playback sealed with SHA-256 and verified; command search across sessions	—	—	✔ Included
List price per privileged user per year	US\$240 · ₹22,840	US\$420 · ₹39,970	US\$660 · ₹62,810
Platforms and coverage			
SSH	Linux/Unix servers and any SSH host		
RDP / VNC	Windows / any VNC server		
Rotation	Linux (server agent), Windows local accounts (desktop agent), PostgreSQL, MySQL		
Console	Modern browser		
Deployment options			

SaaS (India region) with cloud broker	Available Public targets must be in your allowed networks.
Hybrid (private targets)	Partial Through a Secure Access connector node on your network (a binary today); a dedicated on-site gateway is on the roadmap.
On-premises / air-gapped	Available On-premises or fully offline, delivered with our team from one kit.
Licensing	
Priced per	Privileged user per year
Counted	Users allowed to check out credentials or open sessions
Trial	30 days
Editions	Organisations that have PrivilegeVault today through Enterprise keep every tier.
Government profile	Government is a profile, not a separate tier or price list: the Elite 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	A modern browser
Requirement 2	Network reachability from the broker, or a Secure Access connector
Requirement 3	TotalHeal server agent on Linux targets and desktop agent on Windows targets for rotation
Requirement 4	A database login that can change its own password for database rotation

10 Getting started

- A modern browser
- Network reachability from the broker, or a Secure Access connector
- TotalHeal server agent on Linux targets and desktop agent on Windows targets for rotation

- A database login that can change its own password for database rotation

Start a 30 days trial in the TotalHeal console with a Sttitz 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/pam

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.