

Remote Access & Support

Remote support with consent, a second approver and a sealed recording

Consented, recorded remote support for Macs and Windows PCs, and audited shells on Linux servers.



TotalHeal
RemoteLink

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

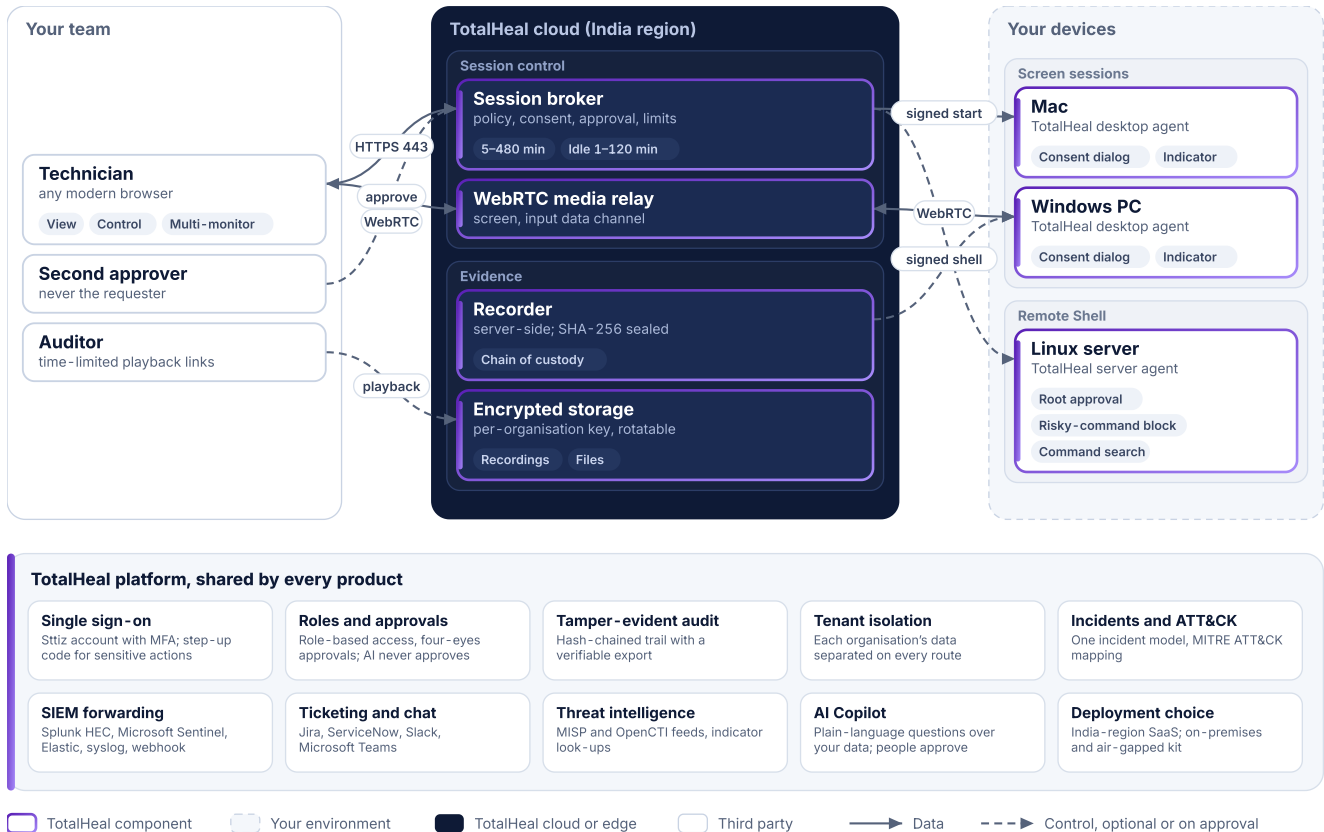
RemoteLink lets IT see and fix a Mac or Windows PC, or open a shell on a Linux server, without an open remote-desktop port or an unaudited third-party tool. The person at the device consents, a second approver can be required, and every session is recorded and sealed.

2 The challenge

IT teams need to see and fix a user's computer, or open a shell on a server, without a permanently open remote-desktop port or an unaudited third-party tool. Auditors want proof of who connected, why, with whose consent and what was done.

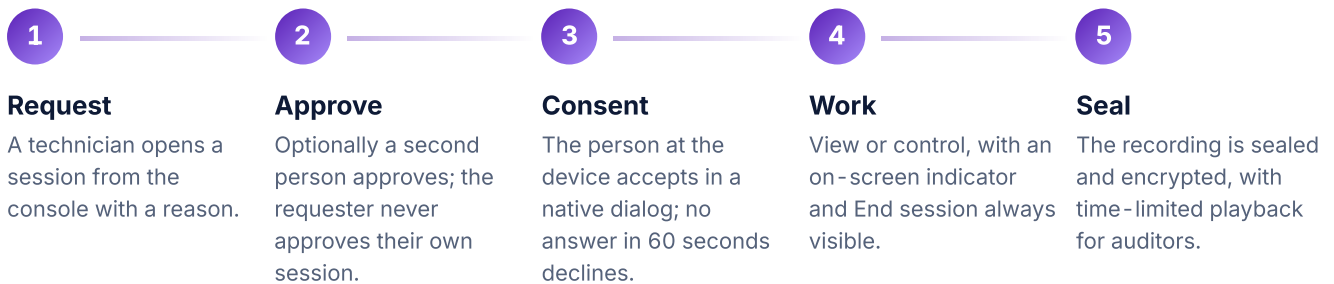
The TotalHeal approach. Screen view or full control from the web console, started only from a signed command over the device's existing outbound channel — no inbound port on the device.

3 Architecture



Sessions start only from a signed command over the device's existing outbound channel; media flows over WebRTC; recordings are sealed and encrypted.

4 How it works



5 Capabilities in detail

- View or control from the browser**
Screen view or full control of an enrolled Mac or Windows PC from the web console.
- Optional second approver**
A second person must approve; the requester can never approve their own session.
- Consent on the device**
A native consent dialog — always on personal devices, on corporate devices unless policy turns it off. No answer in 60 seconds declines.
- Sealed, encrypted recordings**
Server-side recording, sealed with SHA-256 and encrypted at rest with a per-organisation key you can rotate, with chain of custody and time-limited playback links.



Always visible to the person

An on-screen indicator with “End session” for the whole session; keystrokes are never injected into password fields.



Remote Shell for servers

Linux servers (and desktops if enabled): approval for production and root, risky-command blocking, recordings with integrity check and command search.



Finds other remote tools

Detects other remote tools and OS sharing services on the device and offers to turn them off. Every step lands in the hash-chained audit.



Files and clipboard, off by default

File transfer both ways is consented separately, size and type limited, scanned before it is written and encrypted at rest. Clipboard sharing is off by default.



Limits you set

Maximum duration 5–480 minutes, idle timeout 1–120 minutes, one live screen session per device.

The screenshot shows the 'Policy' configuration page for Remote Access. The interface includes a top navigation bar with 'File', 'Home', 'Sessions', 'Remote', 'View', and 'Help'. Below this is a sidebar with 'Start session', 'Sessions', 'Recordings', and 'Policy'. The main content area is titled 'Remote Access Policy' and includes a 'Save policy' button. The policy is divided into several sections:

- Approval and consent:**
 - ☐ **Require a second approver**
Someone with response-approval permission (not the requester) approves every session before the device is asked.
 - ☒ **Ask the person on corporate devices**
Personal (BYOD) devices always ask; this applies to company-owned ones. The on-screen indicator is always shown.
The consent prompt declines on its own after 60 seconds.
- Recording:**
 - ☒ **Record every session**
Recorded server-side and sealed with SHA-256. Turning this off is audited.
The recorder is running.
- What a session may do:**
 - ☒ **Allow control**
Mouse and keyboard. BYOD: only when the person ticks it.
 - ☐ **Allow clipboard sharing**
Text only, both directions. Off by default.
 - ☐ **Allow file transfer**
Off by default. Both directions, through the server (encrypted at rest, deleted once delivered); the person allows it separately for each session and every file is audited with its SHA-256.
- File transfer limits:**
 - Largest file (MB):** 25
 - Only these types (empty = any type that is not blocked):** e.g. .pdf .docx .log .zip
 - Never these types (always wins):** .scr .pif .com .cpl .hta .lnk .vbs .vbe .js .jse .wsf .wsh
Installers stay allowed by default — every file sent to a device is scanned by the TotalHeal engine there before it is written, and a malicious one is refused and raises an alert.
- Limits:**
 - Maximum session length (minutes):** 60
 - End after inactivity (minutes):** 15

Remote Access policy in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

No inbound port

Sessions start only from a signed command over the device's own outbound channel.

Sealed recordings

Recordings are sealed with SHA-256, encrypted per organisation and kept with chain of custody.

Consent and visibility

Consent is always asked on personal devices; the person can end the session at any time.

Files off by default

File transfer and clipboard are off by default, consented separately and scanned.

7 Where it fits

Help desk

Fix a user's laptop with their consent, recorded for quality and audit.

Server shells for admins

Approved, recorded shells on production servers with risky commands blocked.

Retire unmanaged tools

Find other remote tools on devices and replace them.

8 Deployment and system requirements



Cloud (SaaS)

Available

Run by TotalHeal in an India region: nothing to host, updates delivered by us.



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



macOS
11 and later



Windows
10 / 11 (x64)



Linux
servers
Remote Shell

Works with



Any
modern
browser

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

- Enrolled device with the TotalHeal desktop agent (or server agent for shells)
- Outbound HTTPS/WebRTC from the device and the viewer
- The person at the device present to consent (unless the corporate-consent switch is off)

Alerts and tickets to

splunk> Splunk

Microsoft
Sentinel

Elastic

Syslog /
CEF

Jira

ServiceNow

Slack

Microsoft
Teams

9 Technical specifications

Features	Included	
View or control from the browser	✓ Included	
Consent on the device	✓ Included	

Optional second approver	✔ Included	
Sealed, encrypted recordings	✔ Included	
Always visible to the person	✔ Included	
Files and clipboard, off by default	✔ Included	
Remote Shell for servers	✔ Included	
Limits you set	✔ Included	
Finds other remote tools	✔ Included	
Availability by edition		
	Business	Enterprise
Screen sessions, consent, recording, approval, file transfer, clipboard, multi-monitor, Remote Shell	✔ Included	✔ Included
Recording retention options, dual-consent policies	—	Planned
Platforms and coverage		
macOS and Windows desktops	Screen sessions — TotalHeal desktop agent 0.3.4 or later	
Linux servers	Remote Shell — TotalHeal server agent (off until enabled)	
Viewer	TotalHeal web console in a current browser	
Deployment options		
SaaS (India region)	Available	
On-premises	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	Concurrent technician per year	
Counted	Concurrent sessions per technician seat; managed endpoints are not counted	
Trial	30 days	
Editions	Today every Remote Access feature is open at Business; the Enterprise depth above is the commercial plan.	
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	Enrolled device with the TotalHeal desktop agent (or server agent for shells)
Requirement 2	Outbound HTTPS/WebRTC from the device and the viewer
Requirement 3	The person at the device present to consent (unless the corporate-consent switch is off)

10 Getting started

- Enrolled device with the TotalHeal desktop agent (or server agent for shells)
- Outbound HTTPS/WebRTC from the device and the viewer
- The person at the device present to consent (unless the corporate-consent switch is off)

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/remote-access

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.