

Digital Forensics & Triage

Triage evidence collected in minutes, with a chain of custody

Collect triage evidence from an endpoint or server during an investigation, with chain of custody.



TotalHeal
EvidenceLens

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

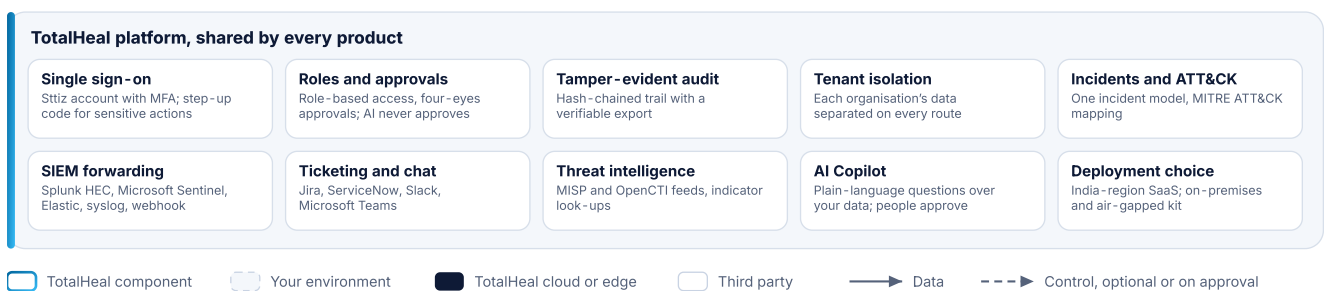
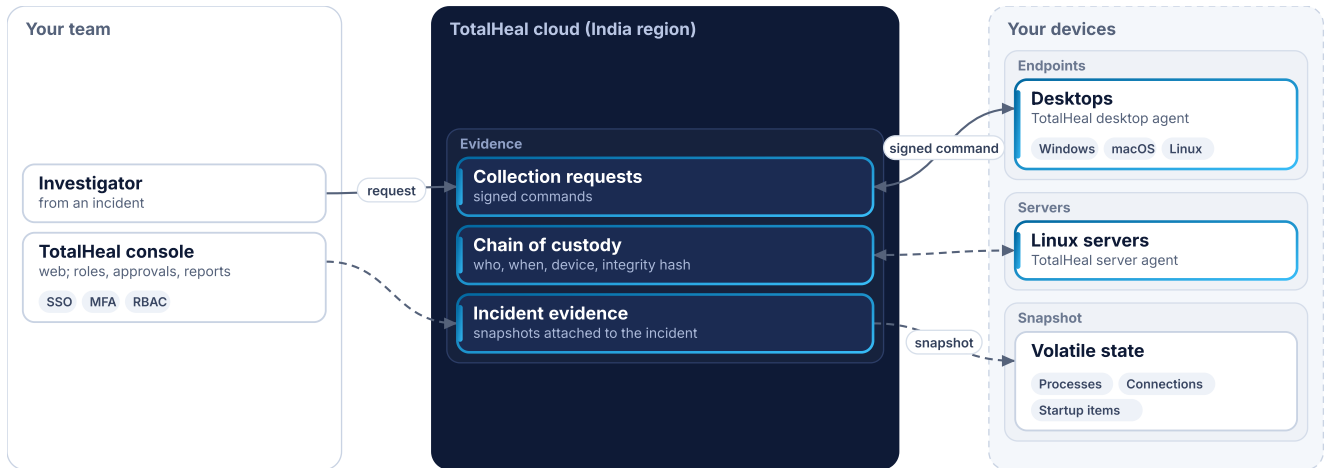
EvidenceLens collects a volatile-state snapshot — running programs, connections, startup items — from an endpoint or server on a signed command, shows the collection to the person at the device, and keeps it with a chain of custody.

2 The challenge

During an incident the first questions are what was running, what was connected and what starts at boot — and the answers vanish when a machine is rebooted or cleaned. Evidence collected ad hoc, by hand, is hard to defend later.

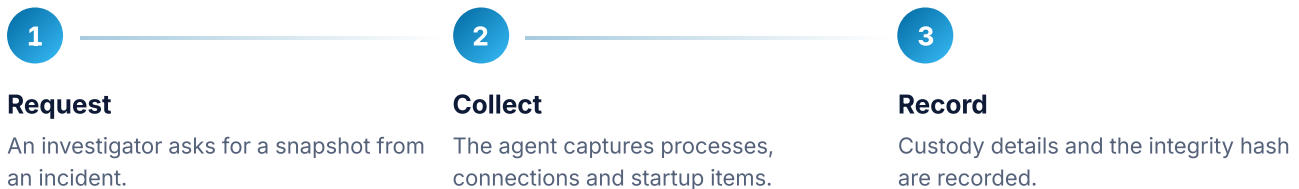
The TotalHeal approach. EvidenceLens takes a volatile-state snapshot from an endpoint or server on a signed command from the console, shows the collection to the person at the device, and keeps the evidence with a chain of custody.

3 Architecture

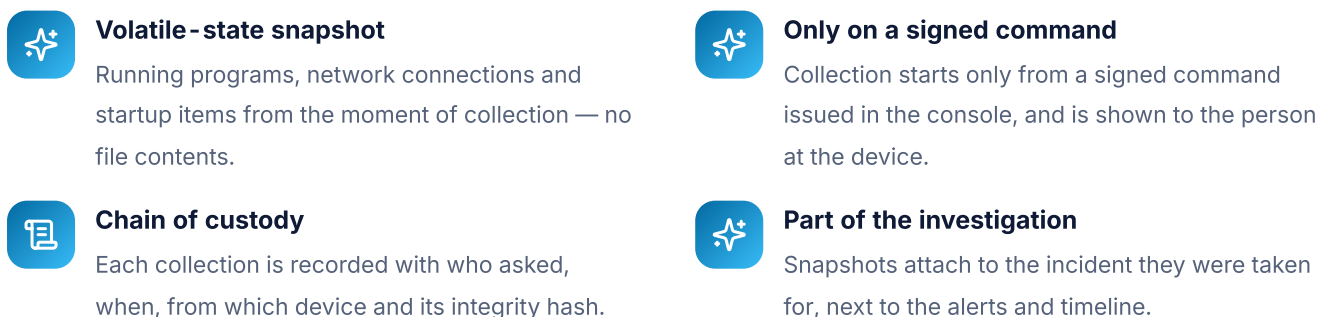


Collection starts only from a signed console command, is shown at the device, and is kept with a chain of custody; snapshots carry no file contents.

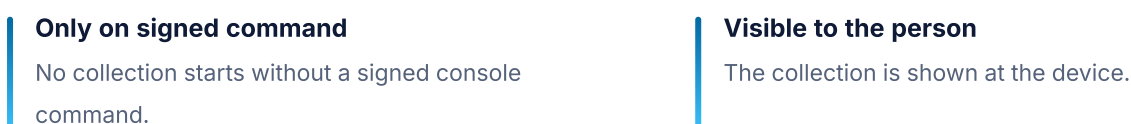
4 How it works



5 Capabilities in detail



6 Security and data handling



No file contents

Snapshots hold lists, not files.

7 Where it fits

First hour of an incident

Capture what is running before anyone reboots.

Defensible evidence

Custody records for later review.

Remote sites

Collect from devices you cannot reach in person.

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



Windows
10 / 11 (x64)



macOS
11 and later



Linux desktop
.deb,
ApplImage



Linux servers
x86_64,
aarch64,
systemd

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 TotalHeal agent on the endpoint or server (any TotalHeal agent licence)
- An EvidenceLens licence

Alerts and tickets to

splunk>

Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams

9 Technical specifications

Features	Included
Volatile-state snapshot	✓ Included

Only on a signed command	✔ Included	
Chain of custody	✔ Included	
Part of the investigation	✔ Included	
Availability by edition		
	Business	Enterprise
Triage snapshots on signed command, chain of custody	✔ Included	✔ Included
Disk and memory acquisition	—	Roadmap
Platforms and coverage		
Windows, macOS, Linux desktops	TotalHeal desktop agent	
Linux servers	TotalHeal server agent	
Console	TotalHeal web console	
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	Endpoint per year	
Counted	Devices that can be collected from	
Trial	30 days	
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	A TotalHeal agent on the endpoint or server (any TotalHeal agent licence)
Requirement 2	An EvidenceLens licence

10 Getting started

- A TotalHeal agent on the endpoint or server (any TotalHeal agent licence)
- An EvidenceLens licence

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/forensics

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.