Endpoint Detection & Response (EDR)

Seeing, investigating and stopping attacks on the servers that run the business

See, investigate and stop attacks on Linux servers today; desktop EDR is in development.



TotalHeal
ThreatTrace

Freaquer Corporation Pvt Ltd

totalhealsecurity.com

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

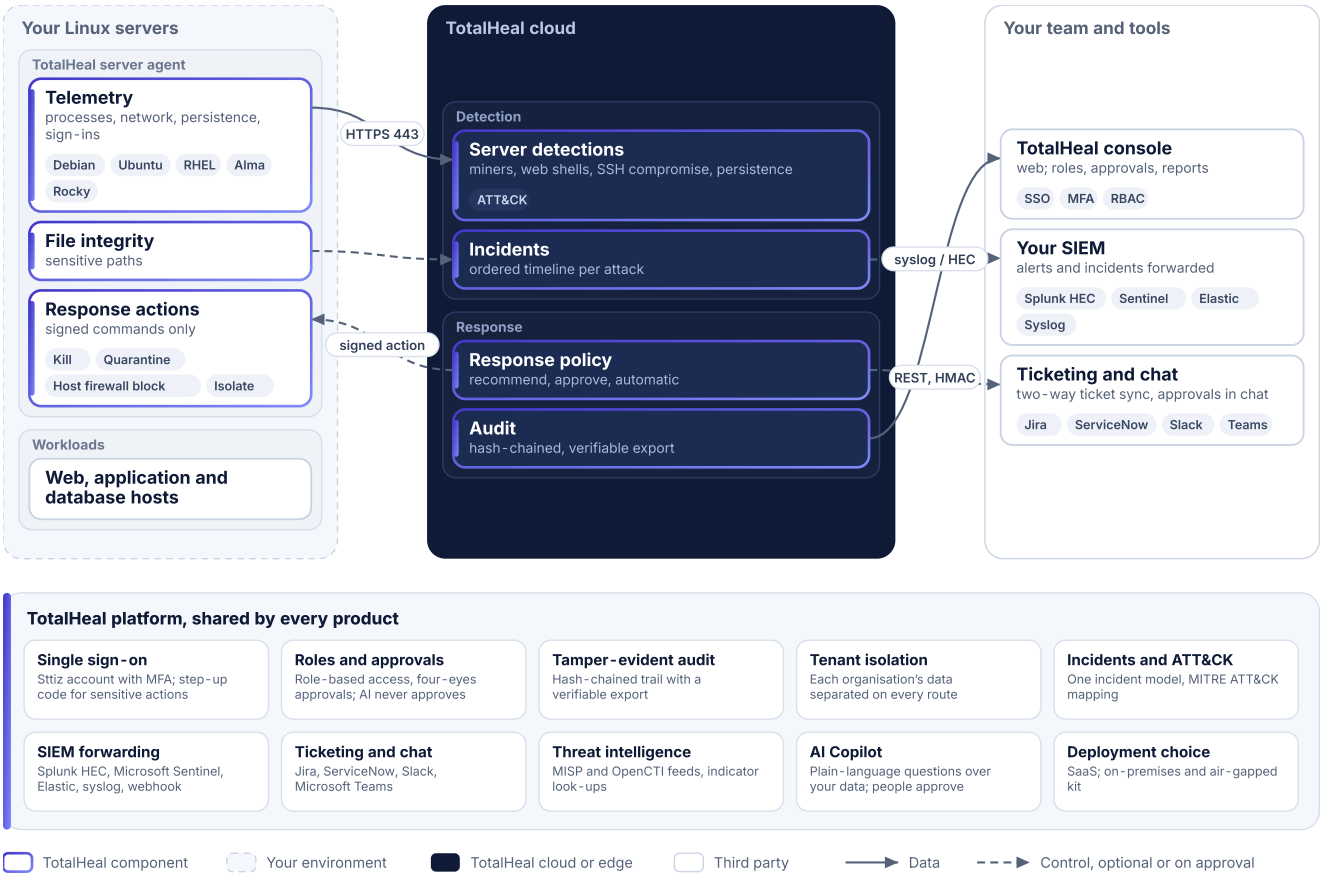
ThreatTrace collects activity on Linux servers, detects the attacks that hit servers — crypto-miners, web shells, SSH compromise — joins them into incidents with a timeline and responds behind your approval rules, with every action on a verifiable audit trail.

2 The challenge

Servers that run the business — web, application and database hosts — are where attackers mine crypto, plant web shells and move in over stolen SSH keys. Antivirus alone does not show what happened, in what order, or stop it with a record of who decided.

The TotalHeal approach. ThreatTrace collects process, network, persistence, file-integrity and sign-in activity on each Linux server, detects attacks mapped to MITRE ATT&CK, joins them into incidents with a timeline, and responds behind your approval rules.

3 Architecture



The server agent collects, detects and responds on the server; the cloud correlates, asks for approval and audits.

4 How it works

1

Collect

Processes, connections, persistence, file integrity and sign-ins.

2

Detect

Server attack patterns mapped to MITRE ATT&CK.

3

Correlate

Related detections become one incident with a timeline.

4

Respond

Kill, quarantine, block or isolate, as your policy allows.

5 Capabilities in detail

Server telemetry

Processes, network connections, persistence (services, cron, startup), file integrity of sensitive paths and sign-ins, from the TotalHeal server agent.

Detections that matter on servers

Crypto-miners, web shells, SSH compromise and suspicious persistence, each mapped to a MITRE ATT&CK technique.

Incidents with a timeline

Related detections are joined into one incident with an ordered timeline of what ran, what connected and what changed.

Response with approval

Kill a process, quarantine a file, block an address in the host firewall or isolate the server — automatic, approved or recommended, as your response policy says.

Tamper-evident audit

Every response request, approval and result lands in a hash-chained audit you can export and verify.

A licence of its own

A ThreatTrace licence alone is enough on a Linux server; no desktop agent and no other TotalHeal product is needed.

6 Security and data handling

Signed commands only

The agent acts only on signed commands from your organisation.

Approval for impact

Isolation and other high-impact actions follow your approval rules.

Verifiable audit

Every request, approval and result on a hash-chained audit.

7 Where it fits

Internet-facing servers

Web shells and miners detected and stopped.

SSH estates

Compromised keys and unusual logins surfaced as incidents.

Servers without desktop tooling

EDR on servers without buying a desktop agent.

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

Network and access

- The TotalHeal server agent on each Linux server
- Outbound HTTPS from each server to the TotalHeal cloud

Alerts and tickets to

- Splunk
- Microsoft Sentinel
- Elastic
- Syslog / CEF
- Jira
- ServiceNow
- Slack
- Microsoft Teams

Software

Nothing to pre-install: no container runtime, database, web server or Java



9 Technical specifications

Features	Included	
Server telemetry	✓ Included	
Detections that matter on servers	✓ Included	
Incidents with a timeline	✓ Included	
Response with approval	✓ Included	
Tamper-evident audit	✓ Included	
A licence of its own	✓ Included	
Availability by edition	**Business**	**Enterprise**
Server telemetry, detections, incidents, response with approval, audit	✓ Included	✓ Included
Platforms and coverage		
Linux servers: Debian, Ubuntu, RHEL, AlmaLinux, Rocky	TotalHeal server agent (signed .deb and .rpm packages)	
Windows, macOS and Linux desktops	In development: not sold for desktops yet	
Console	TotalHeal web console	
Deployment options		
SaaS	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	Linux servers with ThreatTrace switched on	
Trial	30 days	

Editions	No Business/Enterprise split is set for ThreatTrace yet.
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	The TotalHeal server agent on each Linux server
Requirement 2	Outbound HTTPS from each server to the TotalHeal cloud

10 Getting started

- The TotalHeal server agent on each Linux server
- Outbound HTTPS from each server to the TotalHeal cloud

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/edr

Figures are from our own tests where stated, with their dates. Specifications can change; this whitepaper is dated 27 October 2026.