TotalHeal

ThreatTrace

Endpoint Detection & Response (EDR)

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

Cloud (SaaS) | On-premises | Air-gapped

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 answer

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.

Status	**Available**
Deploys as	**Cloud (SaaS) · On-premises · Air-gapped**
Runs on	**Linux servers: Debian, Ubuntu, RHEL, AlmaLinux, Rocky; Windows, macOS and Linux desktops**
Priced per	**Endpoint per year**
Trial	**30 days**
Licence	**Sold on its own; one TotalHeal console**

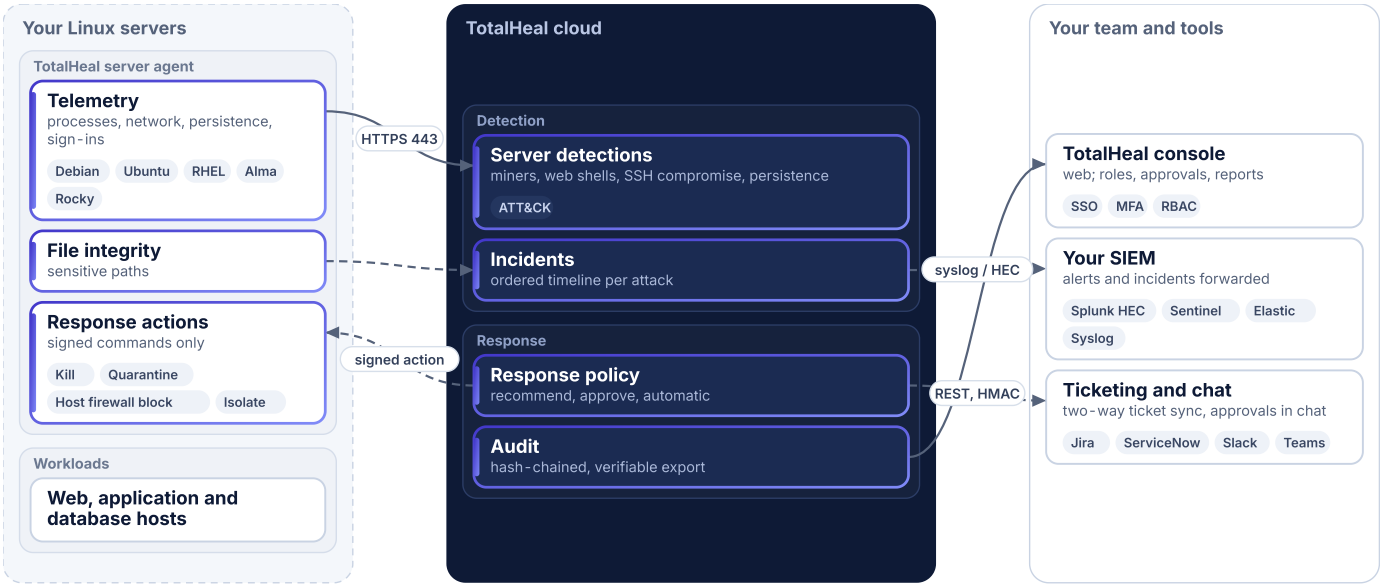
Supported platforms

- **Ubuntu** 20.04, 22.04, 24.04
- **Debian** 11, 12
- **Red Hat Enterprise Linux** 8, 9
- **Rocky Linux** 8, 9
- **AlmaLinux** 8, 9

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.

Reference architecture



TotalHeal platform, shared by every product

Single sign-on Sttiz 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** SaaS; on-premises and air-gapped kit

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

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

Key capabilities

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.

Deployment options

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.

System requirements

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

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



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**

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

Get started

30 days trial in the TotalHeal console. Quotes and the procurement dossier (compliance matrix, bill of materials, architecture and hardening, SLA, OEM authorisation letter): business@totalhealsecurity.com

Freaquer Corporation Pvt Ltd

totalhealsecurity.com/products/edr · whitepaper: totalhealsecurity.com/datasheets/totalheal-edr-whitepaper.pdf?v=fdf0c64a94

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