

Server & Infrastructure Security (hardening and configuration)

Hardened servers that stay hardened — and evidence that they are

Continuously checks how your Linux servers are configured — 79 hardening checks with evidence — and fixes them with a second person's approval and a rollback for every change.



TotalHeal
InfraGuard

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

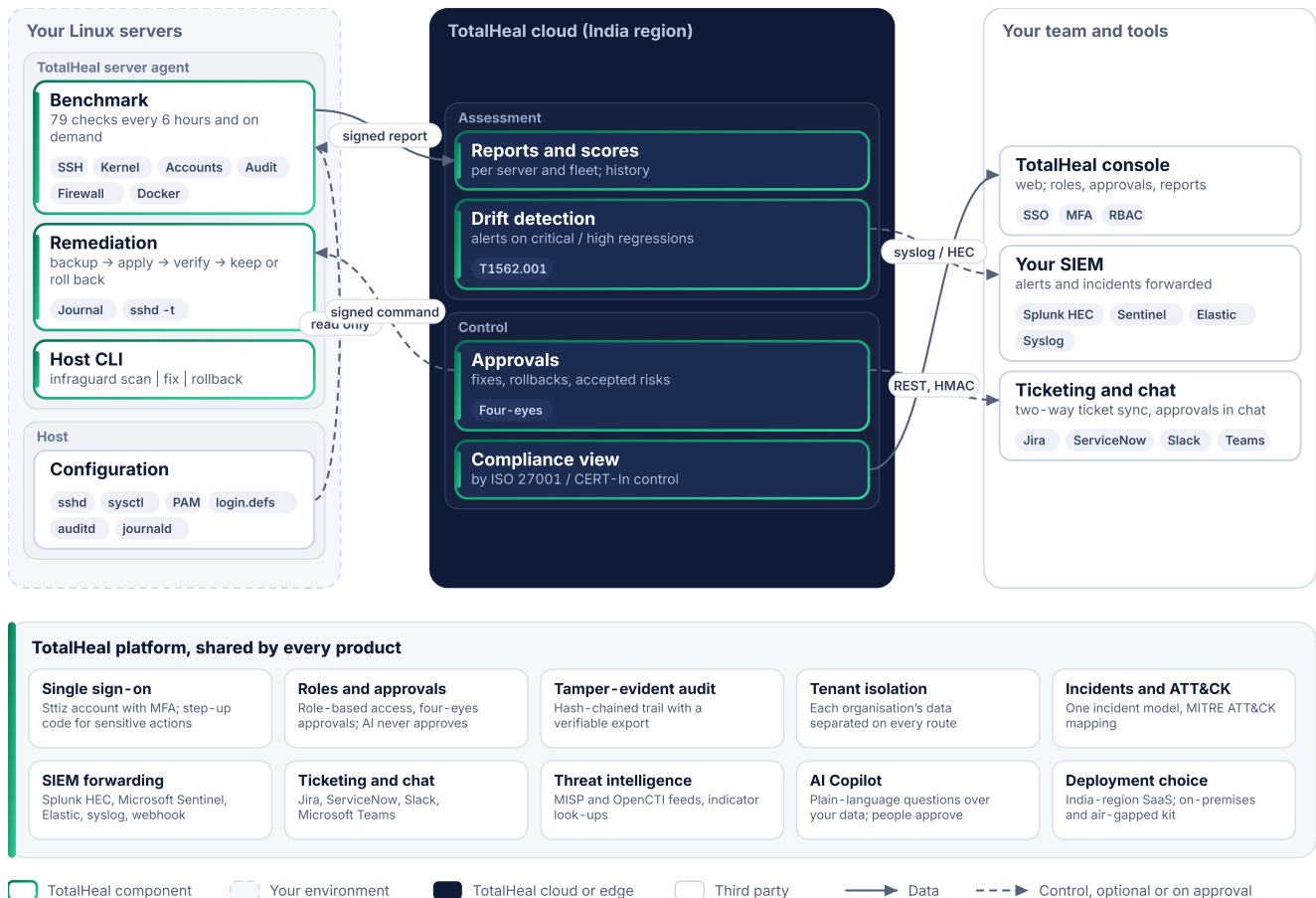
InfraGuard checks every Linux server against 79 hardening checks, shows the exact setting it found, alerts the moment a server drifts, and fixes what a second person approves — backing up every file, checking each fix took effect and keeping a rollback for every change.

2 The challenge

Most server breaches start with a setting, not a zero-day: root logins over SSH, password logins open to the internet, weak ciphers, world-readable shadow files, no audit trail, no firewall. Servers drift — a hardened image is weakened by the next change — and auditors ask for evidence that nobody has.

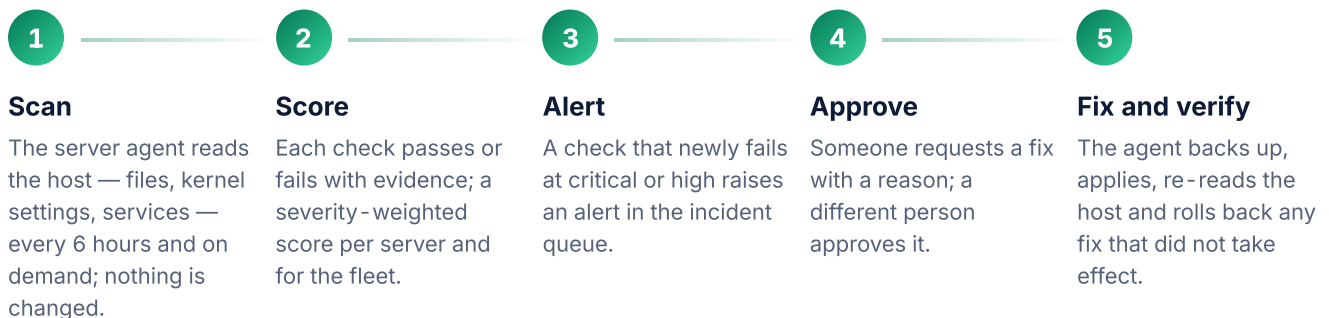
The TotalHeal approach. InfraGuard runs a 79-check hardening benchmark on every Linux server through the TotalHeal server agent, scores each server and the fleet, alerts when a check newly fails, and fixes what you approve — with a backup, a check that the fix took effect, and a rollback for every change.

3 Architecture



The agent reads the server and reports over signed HTTPS; fixes arrive as signed commands only after a second person approves, and every change is journaled on the server.

4 How it works



5 Capabilities in detail

79 checks with evidence

SSH (root and password login, attempts, ciphers, MACs, key exchange, host keys), kernel and network settings, accounts and PAM, file permissions, services, logging and audit, updates, firewall, time sync, SELinux / AppArmor, Secure Boot and Docker — each result with the exact value found.

Why it matters, how to fix

Every check explains the risk in one sentence and names its fix or the guidance to follow.



Score per server and for the fleet

A severity-weighted score from 0 to 100 (critical 10, high 6, medium 3, low 1), score history, and the checks failing on most servers.



Fixes with four-eyes approval

Request a fix with a reason; a second person approves — never the requester, never an AI; the agent applies it as a signed command.



Safe where it matters

SSH changes are validated with `sshd -t` before reload; firewall and partition changes are guidance only, never automatic; remediation runs only where the host owner allowed it.



Evidence by control

Results grouped by ISO 27001:2022 Annex A control and the CERT-In directions (log retention, clock synchronisation) for auditors.



Drift alerts

A check that newly fails at critical or high raises an alert (MITRE ATT&CK T1562.001) in the same incident queue as every other alert.



Backup, verify, roll back

Every file a fix touches is backed up first; the host is re-read to check the fix took effect, and a fix that did not is rolled back automatically. Any applied fix can be rolled back later, byte for byte.



Accepted risks

An exception for one server or all servers needs a reason, an expiry of up to a year and a second person; it leaves the score while it lasts.



On the host too

`totalheal-server-agent infraguard scan | fix | rollback` runs the same benchmark on a server without the cloud.

TotalHeal
Security for what's next

Search anything... (devices, users, apps, policies, vulnerabilities, serial, IP, CVE, ...)

File Home InfraGuard View Help

Overview Servers Approvals Checks Compliance

InfraGuard
Hardening and configuration of your Linux servers — checked continuously, fixed with a second person's approval.

Fleet score **74/100**
0 good · 1 fair · 2 poor

Servers **3**
79 checks each

Critical and high findings **9**
37 medium · 18 low

Servers that regressed **0**
in the last 24 hours

Waiting for approval **1**
1 accepted risks

Failing on most servers Weighted by severity

Check	Severity	Servers	Fix
IG-FW-01 A host firewall is active	high	3	guidance
IG-LOG-01 Audit daemon is running	high	3	automatic
IG-SSH-02 SSH password logins are off (keys only)	high	2	automatic
IG-ACC-08 Accounts lock after repeated failed logins	medium	3	guidance
IG-FS-01 /tmp is a separate mount with nodev, nosuid, noexec	medium	3	guidance
IG-FS-02 /dev/shm has nodev, nosuid, noexec	medium	3	automatic
IG-LOG-02 Changes to accounts, sudo and time are audited	medium	3	automatic
IG-TIM-01 The clock is synchronised	medium	3	automatic
IG-UPD-02 Security updates install	medium	3	automatic

Weakest servers Lowest scores first

Server	OS	Score	Failed
legacy-app-01	CentOS Linux 7 (Core)	68	28
web-01	Ubuntu 22.04.4 LTS	69	26
core-db-01	Ubuntu 22.04.4 LTS	86	9

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

6 Security and data handling

Read-only by default

Scanning never changes a server; fixes run only where the host owner allowed remediation.

Every change can be undone

Files are backed up before a fix and restored byte for byte by a rollback.

Two people for every change

Fixes, rollbacks and accepted risks need a second person; the requester and AI never approve.

No lock-outs

SSH changes are validated before reload; firewall and partition changes are never automatic.

7 Where it fits

Audit evidence

Show ISO 27001 and CERT-In evidence for every server, not a spreadsheet.

Golden images that drift

Know the day a hardened server is weakened by a change.

Fixing at scale

Fix a failing check on every server with one approved request.

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



**Docker
hosts**

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, with `infraguard.enabled`
- `infraguard.allow_remediation` on servers where approved fixes may run
- Outbound HTTPS from each server to the TotalHeal cloud

Alerts and tickets to

splunk> **Splunk**

**Microsoft
Sentinel**

Elastic

**Syslog /
CEF**

Jira

ServiceNow

Slack

**Microsoft
Teams**

Features	Included	
79 checks with evidence	✔ Included	
Why it matters, how to fix	✔ Included	
Score per server and for the fleet	✔ Included	
Drift alerts	✔ Included	
Fixes with four-eyes approval	✔ Included	
Backup, verify, roll back	✔ Included	
Safe where it matters	✔ Included	
Accepted risks	✔ Included	
Evidence by control	✔ Included	
On the host too	✔ Included	
Availability by edition	Business	Enterprise
Benchmark, scores, drift alerts, approved fixes with rollback, exceptions, compliance view, host CLI	✔ Included	✔ Included
Platforms and coverage		
Ubuntu 20.04, 22.04, 24.04	TotalHeal server agent (signed .deb)	
Debian 11, 12	TotalHeal server agent (signed .deb)	
RHEL, Rocky Linux, AlmaLinux 8 and 9	TotalHeal server agent (signed .rpm)	
Docker hosts	Socket permissions, TCP exposure and inter-container traffic checked	
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	Server per year	

Counted	Servers reporting the InfraGuard benchmark
Trial	30 days, up to 5 servers
Editions	InfraGuard is sold on its own, outside the editions.
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	The TotalHeal server agent on each Linux server, with <code>infraguard.enabled</code>
Requirement 2	<code>infraguard.allow_remediation</code> on servers where approved fixes may run
Requirement 3	Outbound HTTPS from each server to the TotalHeal cloud

10 Getting started

- The TotalHeal server agent on each Linux server, with `infraguard.enabled`
- `infraguard.allow_remediation` on servers where approved fixes may run
- Outbound HTTPS from each server to the TotalHeal cloud

Start a 30 days, up to 5 servers 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/infraguard

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.