

Unified Endpoint Management (UEM)

One record, one policy engine and one signed channel for every device you own

Enrol, configure, update and secure every laptop, phone and tablet from one console.



TotalHeal
DeviceSphere

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

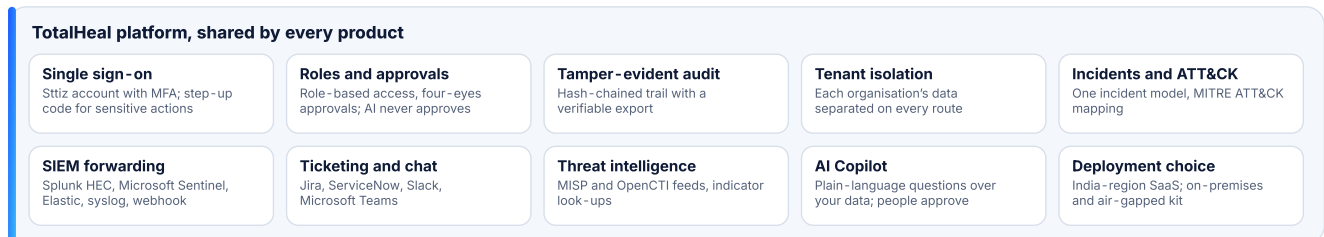
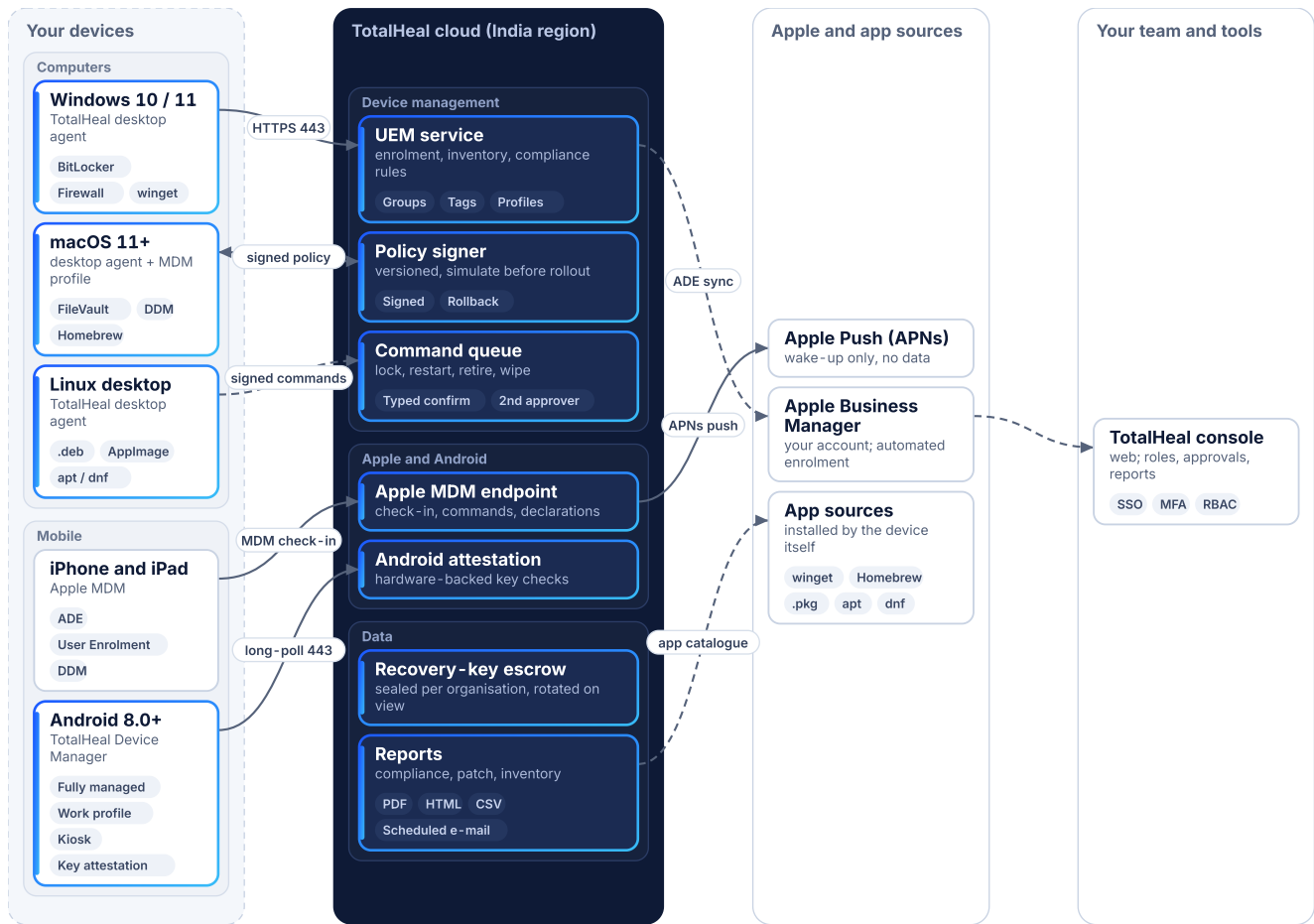
DeviceSphere UEM manages Windows, macOS and Linux computers, iPhones, iPads and Android devices from one console. Every policy and command is signed, destructive actions need a second person, and recovery keys are sealed per organisation — so device management stops being one more way in.

2 The challenge

Organisations run a mix of Windows and Mac laptops, Linux machines, iPhones, iPads and Android phones. IT needs to know what each device is, keep it configured and encrypted, deploy apps, and lock or wipe a lost device — usually with several separate tools.

The TotalHeal approach. One device record, one console, one policy engine and one signed command channel for Windows, macOS, Linux, iPhone, iPad and Android.

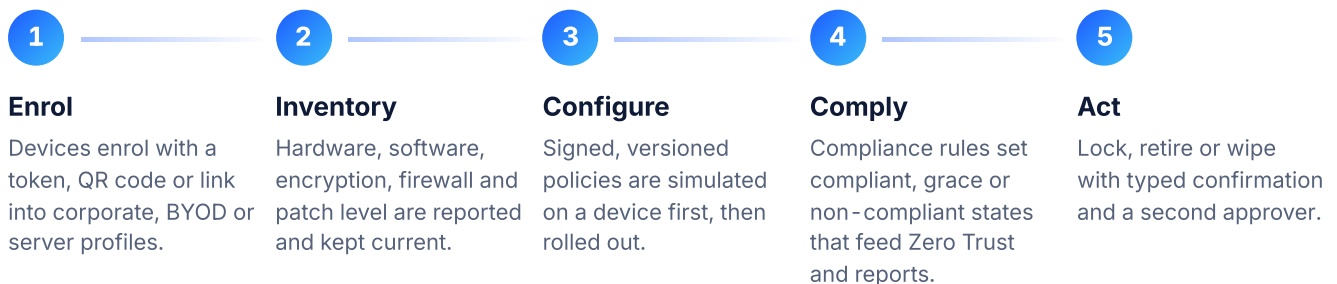
3 Architecture



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

Desktops and Android check in over outbound HTTPS 443; Apple devices through Apple Push; no inbound port on any device or network.

4 How it works





Enrolment your way

Token, QR code or link, with corporate, BYOD and server profiles, groups, tags, expiry and maximum uses. Command-line enrolment for bulk rollout.



Signed configuration policies

Password and screen lock, disk encryption, firewall, OS auto-update, USB control, remote-login services, Wi-Fi rules and settings lock — versioned, with "simulate on device" before rollout.



Apps and updates

An app catalogue deployed through winget, Homebrew/.pkg, apt and dnf, required or self-service, with allow and block rules on the device. OS and third-party updates with patch rings.



Recovery-key escrow

BitLocker and FileVault keys sealed per organisation. Viewing one needs an admin role, a reason and a fresh two-step code; the key is then rotated.



Reports and a tamper-evident trail

Fleet compliance and patch reports as PDF, HTML or CSV, scheduled by e-mail, and a hash-chained audit trail you can verify.



Hardware and software inventory

Model, serial, CPU, RAM, disks, battery, OS and patch level, installed software, users, network, encryption, firewall and Secure Boot.



Compliance rules

Compliant, non-compliant and grace states that feed Zero Trust posture and reports.



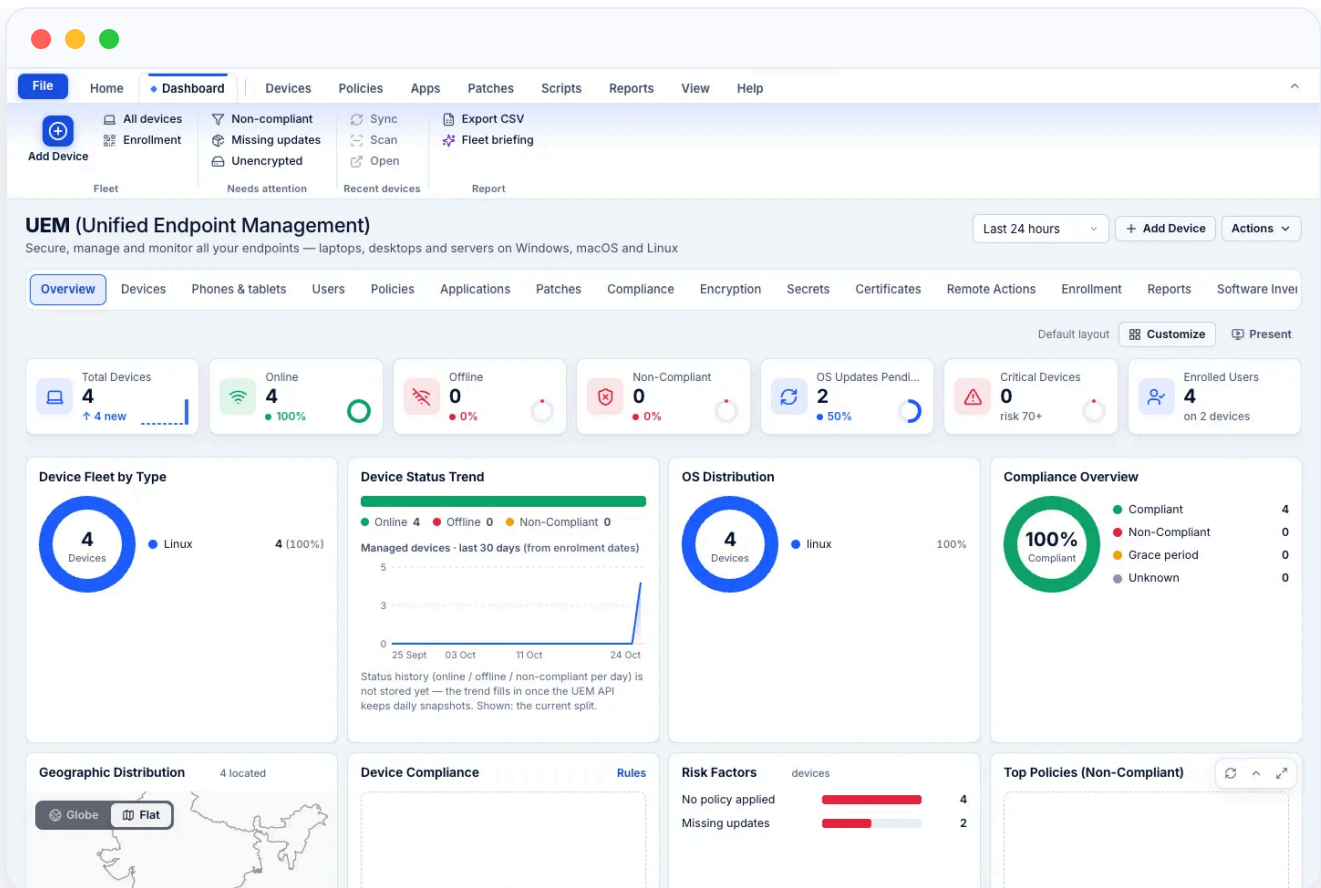
Remote actions with a second approver

Lock, restart, sync, message, collect diagnostics, locate (opt-in) and retire. Destructive actions need a typed confirmation and a second human approver — never AI.



iPhone, iPad and Android

Apple MDM with Declarative Device Management, User Enrolment and Apple Business Manager. An Android device-policy app for fully managed, work profile and kiosk devices, with hardware key attestation.



The UEM dashboard in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

Every command is signed

Devices act only on signed policies and commands from your organisation.

Recovery keys sealed

Viewing a BitLocker or FileVault key needs an admin role, a reason and a fresh two-step code; the key is then rotated.

Two people for destructive actions

Wipe and retire need a typed confirmation and a second human approver — never AI.

A trail you can verify

Every action is on a hash-chained audit trail.

7 Where it fits

Mixed fleets

Windows, Mac and Linux laptops with company phones and tablets under one set of policies.

Lost or stolen devices

Lock, locate (opt-in) and retire, with recovery keys kept safe.

Audit evidence

Encryption, patch and compliance reports scheduled to auditors.

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

Android works over the local network; iPhone and iPad management uses Apple Push.

Protected platforms



Windows
10 / 11 (x64)



macOS
11 and later



Linux desktop
.deb, AppImage



iPhone, iPad
Apple MDM



Android
8.0 and later

Works with



Apple Business Manager

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

- HTTPS from devices to the TotalHeal cloud
- Apple Push certificate for iPhone/iPad
- Android: a factory - reset device for device - owner modes
- A Sttiz account for each console user

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included	
Enrolment your way	✓ Included	
Hardware and software inventory	✓ Included	
Signed configuration policies	✓ Included	
Compliance rules	✓ Included	
Apps and updates	✓ Included	
Remote actions with a second approver	✓ Included	

Recovery - key escrow	✔ Included	
iPhone, iPad and Android	✔ Included	
Reports and a tamper - evident trail	✔ Included	
Availability by edition		
	Business	Enterprise
Enrolment, inventory, policies, apps, compliance rules, remote actions, scripts, Apple MDM, Android, reports	✔ Included	✔ Included
ADE at scale, recovery -key escrow, multi - site, four - eyes policy change	Planned for Enterprise	✔ Included
Windows Autopilot	Roadmap	Roadmap
Platforms and coverage		
macOS 11 and later	TotalHeal desktop agent	
Windows 10 and 11 (x64)	TotalHeal desktop agent	
Linux desktop (.deb, Appliance)	TotalHeal desktop agent — a few actions are macOS/Windows only	
iPhone and iPad	Apple MDM — needs your Apple Push certificate; ADE needs Apple Business or School Manager	
Android 8.0 and later	TotalHeal Device Manager, provisioned by QR code or NFC	
Deployment options		
SaaS (TotalHeal cloud, India region)	Available	
On - premises	Available Delivered with our team from the on - premises kit.	
Air - gapped	Available Android works over the local network; iPhone and iPad management uses Apple Push.	
Licensing		
Priced per	Managed device per year	
Counted	Active enrolled devices: desktops, Apple MDM and Android devices	
Trial	30 days, up to 25 devices	
Editions	The Business/Enterprise split is the commercial plan; until it is enforced, both tiers get the full product.	

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	HTTPS from devices to the TotalHeal cloud
Requirement 2	Apple Push certificate for iPhone/iPad
Requirement 3	Android: a factory-reset device for device-owner modes
Requirement 4	A Sttiz account for each console user

10 Getting started

- HTTPS from devices to the TotalHeal cloud
- Apple Push certificate for iPhone/iPad
- Android: a factory-reset device for device-owner modes
- A Sttiz account for each console user

Start a 30 days, up to 25 devices 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/uem

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.