

Patch Management

Patching in waves, inside working rules, with proof afterwards

See what is missing on every computer and roll updates out in waves — with proof afterwards.



TotalHeal
PatchPilot

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

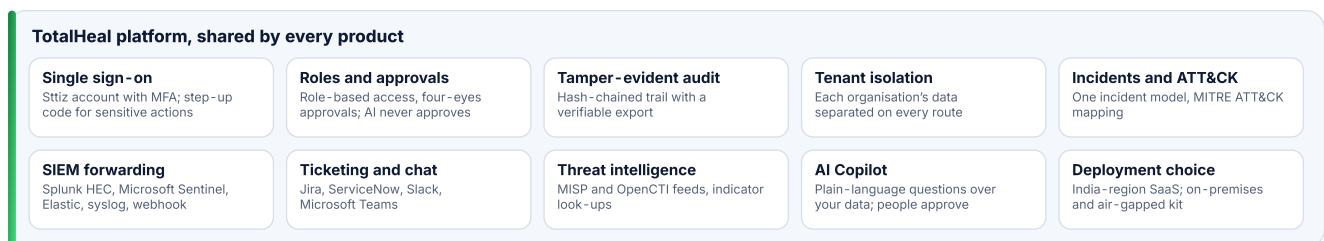
PatchPilot shows what is missing on every computer, rolls updates out in rings with maintenance windows and approvals, and records every install as a signed, audited command — so patching is fast, predictable and provable.

2 The challenge

Unpatched operating systems and applications are the commonest way in. IT teams need to see what is missing on every computer, roll updates out in waves (test group first), respect working hours and prove afterwards that it was done.

The TotalHeal approach. Missing - updates reports, patch rings, maintenance windows and approvals for Windows, macOS and Linux — every install a signed, audited command.

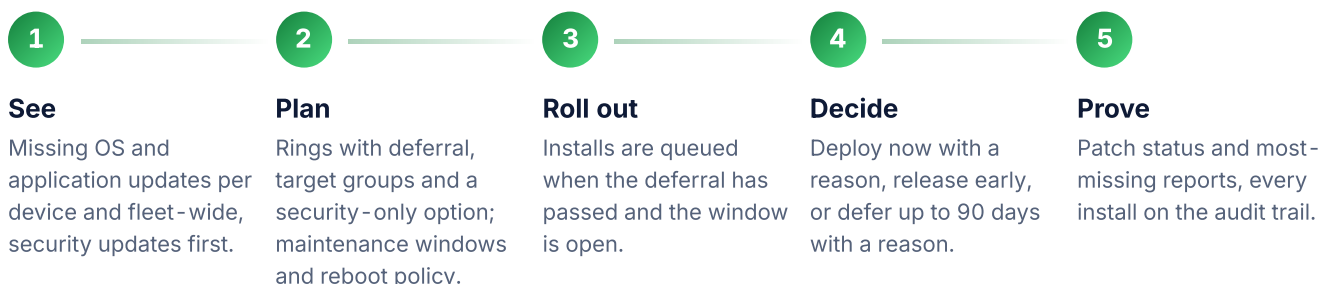
3 Architecture



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

TotalHeal decides what, where and when; devices download from their usual update sources; every install is a signed, audited command.

4 How it works



5 Capabilities in detail





Maintenance windows and reboot policy

Days, start time and 1–24 hour duration; reboot automatically in the window, ask the user, or never.



Deploy now, approve, defer

Deploy selected updates with a mandatory reason, release one without waiting, or defer up to 90 days with a reason.



Drivers and firmware

Windows Update drivers and Linux firmware updates from the device page.



Consent and proof

End users can postpone a limited number of times (default 3). Every install goes through approval levels and the hash-chained audit; “Patch status” and “Most-missing updates” reports.



Automatic ring deployment

Installs are queued when the deferral has elapsed and the window is open, at most once per device per day.



Native installers

Windows Update, macOS softwareupdate, and apt/dnf on Linux. Linux servers get security-only updates by default and are never rebooted by us.



Third-party apps

Updates through winget, Homebrew, apt and dnf for the apps in your organisation catalogue.

UEM > Patch management

Patch management

Missing OS and app updates, patch rings and maintenance windows

+ New patch ring CSV

Overview Devices Phones & tablets Users Policies Applications **Patches** Compliance Encryption Secrets Certificates Remote Actions Enrollment Reports Software Inver

Missing updates 3 Rings & windows 0

Missing updates 3 Devices affected 0 High / critical 3 CVEs fixed by these 0

Missing updates OS and apps

Update	Device	Kind	Severity	CVEs	Released	Decision
☐ git git ? → 2.43.5	1 devices	OS	High	—	—	Ring
☐ linux-image linux-image ? → 6.8.0-49	1 devices	OS	High	—	—	Ring
☐ openssl openssl ? → 3.0.15	1 devices	OS	High	—	—	Ring

Tick updates, then **Deploy now**, **Approve** (rings release it without waiting for their deferral) or **Defer** in the ribbon. Driver and firmware updates: **Update Drivers** on a Windows or Linux device (Windows Update drivers, fwupd firmware).

Patch management in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

Native installers only

Updates come from Windows Update, Apple and your distribution or package managers — never repackaged.

Every install is signed and audited

Each install is a signed command with an approval level and an audit entry.

Servers are not rebooted

Linux servers get security-only updates by default and are never rebooted by TotalHeal.

7 Where it fits

Monthly patch cycles

Pilot ring first, broad ring after a deferral, inside agreed windows.

Emergency CVEs

Push one security update now, with a reason, to the devices that need it.

Audit

Show auditors what was missing, when it was installed and who decided.

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

Devices update from your internal sources (WSUS or local mirrors).

Protected platforms



Windows
10 / 11 (x64)



macOS
11 and later



Linux desktop
.deb,
ApplImage



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

Network and access

- TotalHeal desktop agent or Linux server agent enrolled to your organisation
- Devices can reach their own update sources (Windows Update or WSUS, Apple, distribution mirrors)
- A TotalHeal DeviceSphere UEM entitlement (today)

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

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



9 Technical specifications

Features	Included	
Missing - updates report	✔ Included	
Patch rings	✔ Included	
Maintenance windows and reboot policy	✔ Included	
Automatic ring deployment	✔ Included	
Deploy now, approve, defer	✔ Included	
Native installers	✔ Included	
Drivers and firmware	✔ Included	
Third - party apps	✔ Included	
Consent and proof	✔ Included	
Availability by edition	Business	Enterprise
Missing - updates report, deploy now, CSV	✔ Included	✔ Included
Rings, maintenance windows, reboot policy	Included today	✔ Included
Approve / defer workflow	Included today	✔ Included
Driver and firmware updates	Included today	✔ Included
Platforms and coverage		
Windows, macOS, Linux desktops	TotalHeal desktop agent	
Debian/Ubuntu and RHEL - family servers	TotalHeal Linux server agent	
iPhone, iPad, Android OS updates	Through TotalHeal DeviceSphere UEM, not this product	
Deployment options		
SaaS (TotalHeal cloud, India region)	Available	

On-premises	Available Delivered with our team from the on-premises kit.
Air-gapped	Available Devices update from your internal sources (WSUS or local mirrors).
Licensing	
Priced per	Managed device per year
Counted	Devices with patching switched on
Trial	30 days
Editions	The commercial plan moves rings, drivers/firmware and approval workflows to Enterprise later; the final split is still open.
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	TotalHeal desktop agent or Linux server agent enrolled to your organisation
Requirement 2	Devices can reach their own update sources (Windows Update or WSUS, Apple, distribution mirrors)
Requirement 3	A TotalHeal DeviceSphere UEM entitlement (today)

10 Getting started

- TotalHeal desktop agent or Linux server agent enrolled to your organisation
- Devices can reach their own update sources (Windows Update or WSUS, Apple, distribution mirrors)
- A TotalHeal DeviceSphere UEM entitlement (today)

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/patch-management

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.