

Vulnerability Management

Fixing the vulnerabilities that are actually being exploited, first

Know which installed software carries a known, exploited vulnerability — without a scanner appliance.



TotalHeal
VulnSight

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

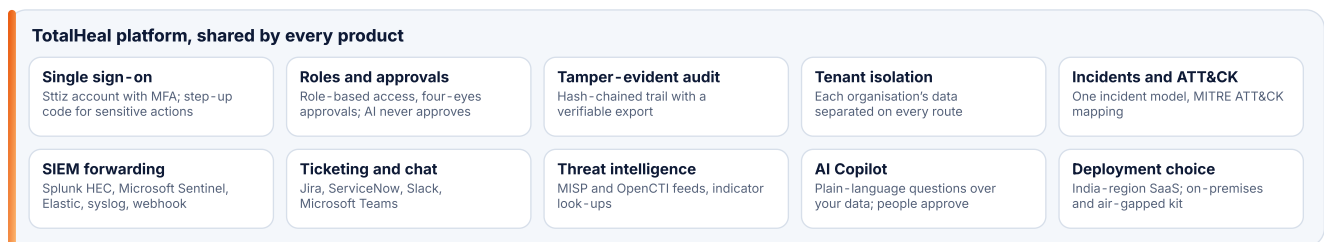
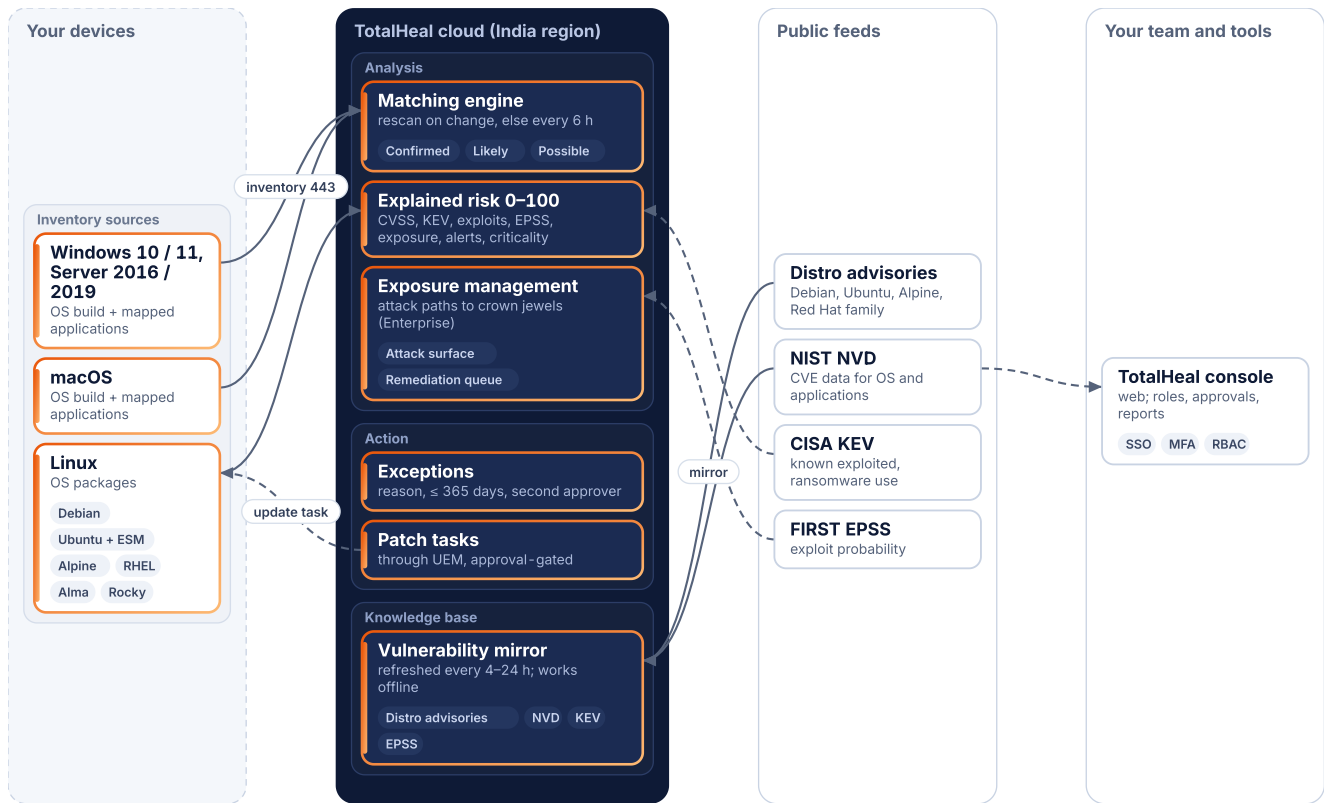
VulnSight matches the software inventory TotalHeal agents already report against a mirrored vulnerability knowledge base. Every finding has a confidence level and an explained 0–100 risk score built from exploitation evidence, so teams fix what attackers use — without a scanner appliance or stored credentials.

2 The challenge

Teams cannot patch everything. They need to know which installed software on which device carries a known vulnerability, which are actually being exploited, and which open a path to their most important systems — without deploying a scanner appliance or handing out admin credentials.

The TotalHeal approach. Agentless matching on the TotalHeal server: the software inventory the TotalHeal agent already reports is matched against a mirrored vulnerability knowledge base. Nothing extra runs on the endpoint and no scanning credentials are stored.

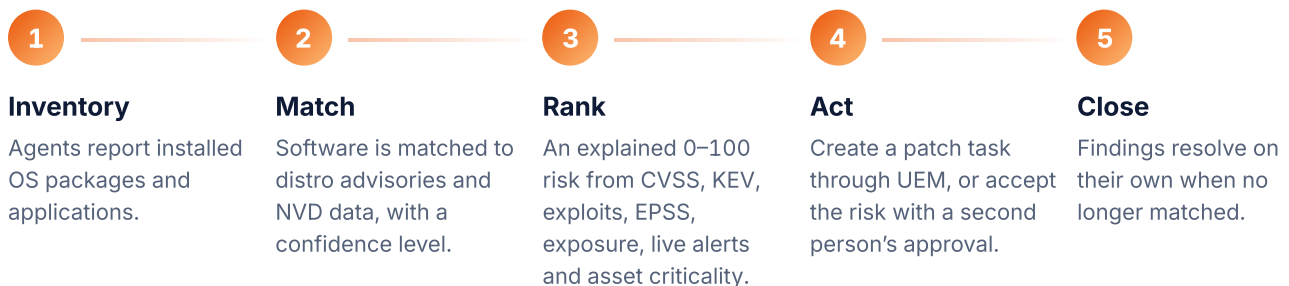
3 Architecture



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

Matching runs in the TotalHeal cloud against mirrored public feeds; nothing extra runs on endpoints and no scanning credentials exist.

4 How it works



5 Capabilities in detail



Linux distro advisories

Debian, Ubuntu (including Ubuntu Pro ESM fixes), Alpine, Red Hat, AlmaLinux and Rocky Linux packages matched against distro advisories.



Confidence on every finding

Confirmed, likely or possible — “possible” is shown apart and never counted.



Explore and graph

CVE explorer, per-device view, CVE detail and a graph from device to software to CVE to ATT&CK technique.



From finding to fix

“Create patch task” raises an update request through UEM — nothing changes automatically. Findings resolve by themselves when no longer matched.



Windows, macOS and desktop apps

OS builds and about 98 curated desktop applications matched against NVD data. Unmapped apps are reported as “not assessed”, never guessed.



An explained 0–100 risk score

CVSS, CISA KEV (including ransomware use), public exploits, FIRST EPSS, internet exposure, live alerts naming the CVE and asset criticality.



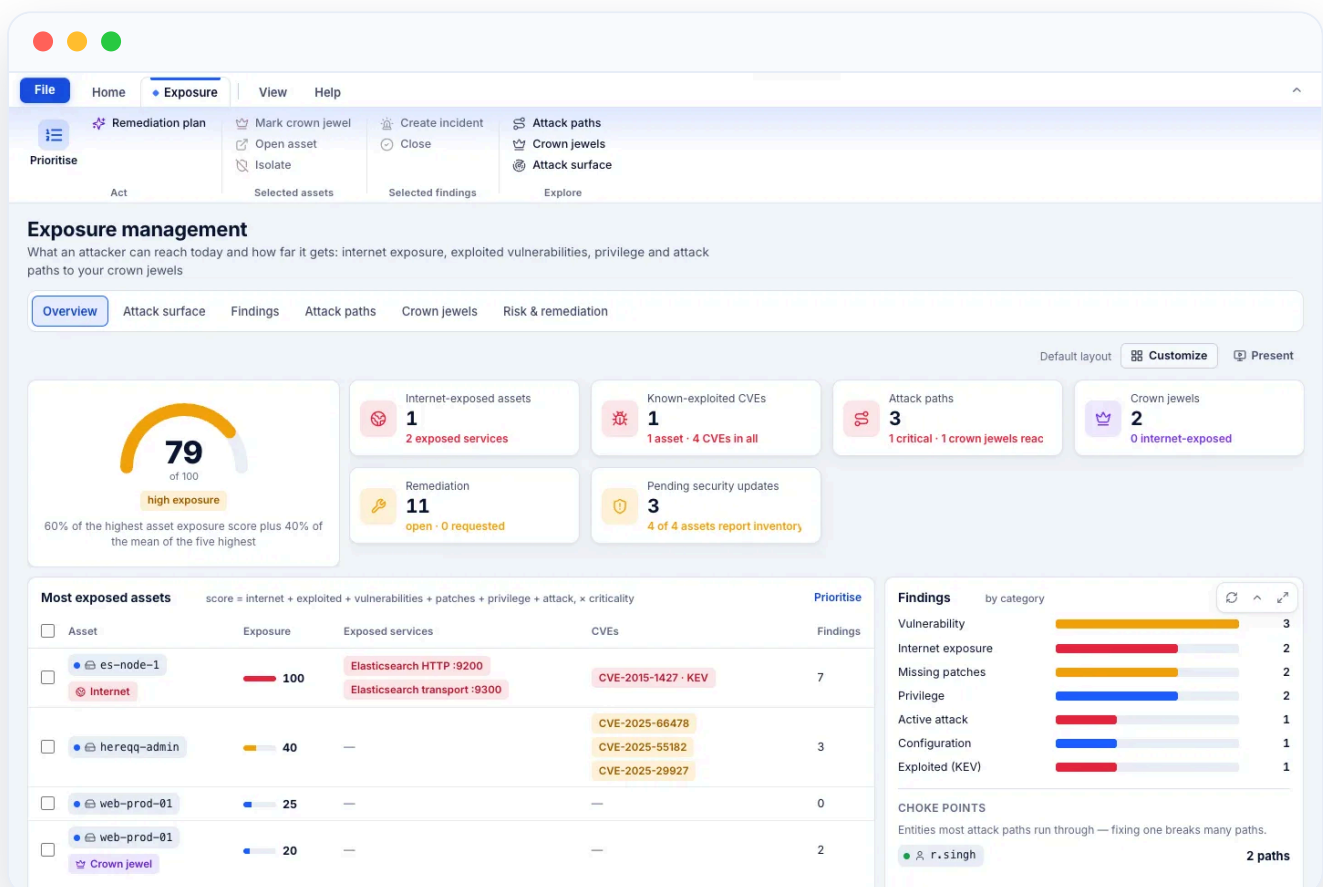
Risk acceptance with a second person

Exceptions need a reason and an expiry of at most 365 days, are approved by a different person, revocable and audited.



Exposure management (Enterprise)

Asset exposure score, attack surface, attack paths to crown jewels, crown-jewel tagging and a remediation queue.



Exposure management, the Enterprise view of Vulnerability Management (demo organisation). Real screenshot, demo data.

6 Security and data handling

No scan credentials

Nothing is scanned remotely and no administrator credentials are stored.

Nothing changes on its own

Patch tasks go through approval; exceptions need a second person and expire.

Never guessed

Unmapped applications are reported as not assessed; possible matches are shown apart and never counted.

7 Where it fits

Exploited - first patching

A weekly queue of known - exploited vulnerabilities on your devices.

Crown jewels (Enterprise)

Attack paths and exposure scores toward the systems you tag as critical.

Risk acceptance on record

Time - boxed exceptions with reasons and approvers for 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

The vulnerability feeds and the control plane run offline.

Protected platforms



Windows
10 / 11 (x64)



Windows Server
2016 / 2019



macOS
11 and later



Ubuntu
20.04, 22.04, 24.04



Debian
11, 12



Red Hat Enterprise Linux
8, 9



Rocky Linux
8, 9



AlmaLinux
8, 9



Alpine

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

- A software - inventory source: today the TotalHeal agent (desktop or Linux server) with its UEM module enabled
- Recommended: Patch Management to act on findings
- 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	
Linux distro advisories	✓ Included		
Windows, macOS and desktop apps	✓ Included		
Confidence on every finding	✓ Included		
An explained 0–100 risk score	✓ Included		
Explore and graph	✓ Included		
Risk acceptance with a second person	✓ Included		
From finding to fix	✓ Included		
Exposure management (Enterprise)	✓ Included		
Availability by edition		Business	Enterprise
CVE matching, confidence, explained risk, KEV / EPSS / CVSS	✓ Included		✓ Included
CVE explorer, device view, graph, data sources	✓ Included		✓ Included
Exceptions with second-person approval	✓ Included		✓ Included
Patch task through UEM	Included (needs UEM)	Included (needs UEM)	
Exposure score, attack surface, attack paths, crown jewels, remediation queue	—		✓ Included
Platforms and coverage			
Linux: Debian, Ubuntu, Alpine, RHEL, AlmaLinux, Rocky	OS packages		
Windows 10/11, Windows Server 2016/2019	OS build and mapped applications		
macOS	OS build and mapped applications		
iOS, Android, network devices, containers, language packages	Not assessed		
Deployment options			
SaaS (India region)	Available		

On-premises	Available Delivered with our team from the on-premises kit.
Air-gapped	Available The vulnerability feeds and the control plane run offline.
Licensing	
Priced per	Asset per year
Counted	Devices reporting a software inventory
Trial	30 days
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	A software-inventory source: today the TotalHeal agent (desktop or Linux server) with its UEM module enabled
Requirement 2	Recommended: Patch Management to act on findings
Requirement 3	A Sttiz account for each console user

10 Getting started

- A software-inventory source: today the TotalHeal agent (desktop or Linux server) with its UEM module enabled
- Recommended: Patch Management to act on findings
- A Sttiz account for each console user

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/vulnerability-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.