

Zero Trust Network Access (ZTNA)

Replacing the VPN with access that shrinks the moment risk rises

Access to named apps and servers only, re-checked continuously — not the whole subnet.



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

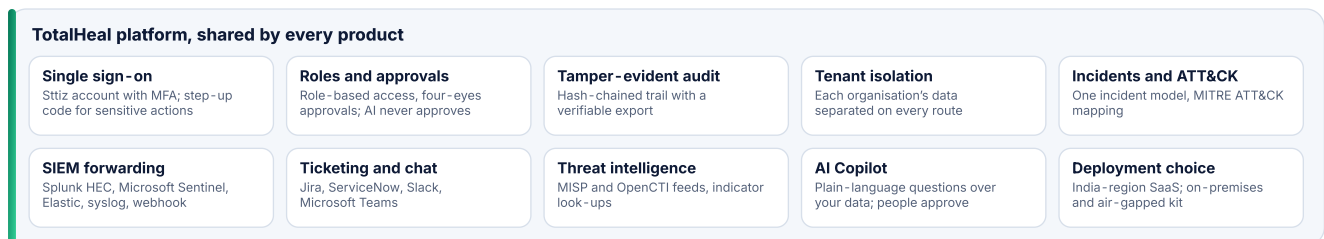
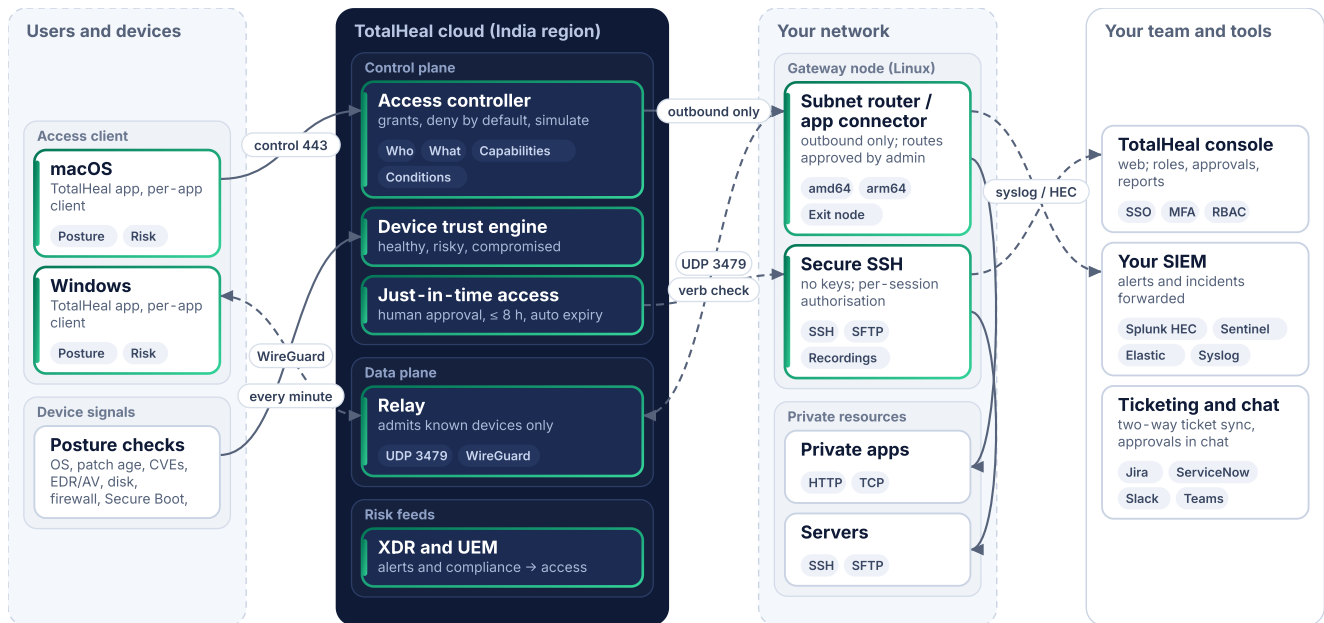
A VPN checks a device once and then trusts it with a whole subnet. ZeroGate grants each user and device access to named applications and servers only, re-evaluates device health and risk continuously, and cuts or narrows access within seconds when a device turns risky — with no inbound port on your network.

2 The challenge

A classic VPN puts a user on the whole subnet and checks the device once, at login. A compromised laptop keeps its access until someone notices.

The TotalHeal approach. Each user and device gets access only to the applications and servers a policy allows, and device health and risk are re-evaluated continuously. When a device's risk rises, its access shrinks or is cut within seconds.

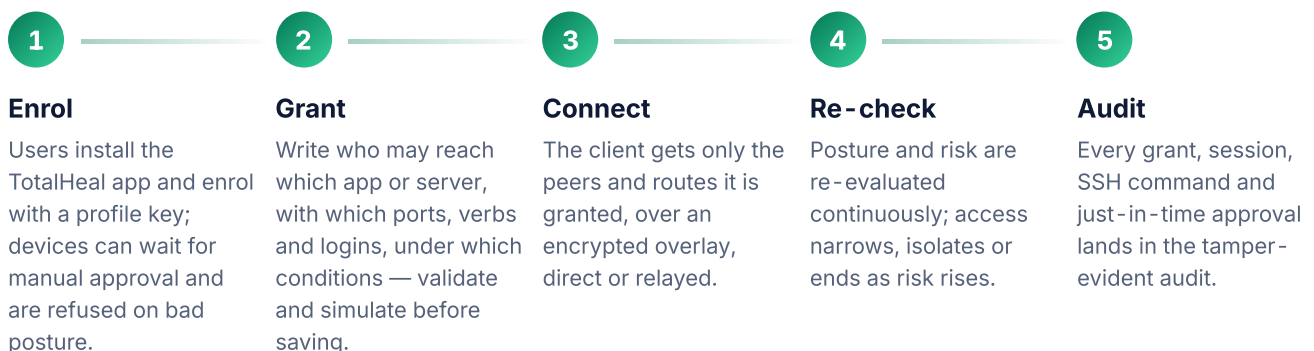
3 Architecture



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

Clients and gateways dial out to the controller; traffic flows over an encrypted WireGuard overlay, peer to peer or through the India relay; no inbound port anywhere.

4 How it works



5 Capabilities in detail

Grants, deny by default
Who (user, group, tag, device, profile) may reach what (app, tag, device, subnet, host), with which capabilities (protocol, ports, HTTP verbs, SSH logins) and under which conditions (posture, risk, MFA age, time, country). Validate and simulate before you save.

A private encrypted network per organisation
Each organisation has its own overlay network; a device only sees the peers and routes it is granted.



Device posture

OS supported, patch age, critical CVEs, rooted, EDR and AV healthy, disk encryption, firewall, Secure Boot, UEM enrolment, certificate and MFA give a healthy, risky or compromised verdict.



Enrolment profiles and approval

Nine profile kinds, one-time or reusable keys, a manual approval queue and automatic rejection on bad posture.



Gateways for private apps

A Linux node as subnet router, exit node or app connector for private HTTP/TCP apps; routes approved by an admin.



Micro-segmentation and response

Deny guards between tags, environments and departments. XDR can revoke access or quarantine a device while a forensic channel stays open.



Risk-adaptive access

Full, restricted, sensitive apps blocked, isolated or quarantined as risk rises. In our tests a high-risk device lost its connections in under a second.



Just-in-time access

Request, automated risk analysis, human approval (never your own), a time-boxed grant (default up to 8 hours) and automatic expiry.



Secure SSH

Identity-based SSH and SFTP with no distributed keys, per-session authorisation, recordings (always on for root) and a searchable command audit.

Secure Access - Grants
Who may reach what, with which capabilities, under which device and identity conditions — deny by default

← All grants **New grant** Simulate Create grant

0 Grant

Name *
Engineering -> staging SSH ☒ Enabled

Description

1 Who source selectors — any of them

Sources
user:ana@example.com, group:engineering, tag:ci, device:<id>, profile:<id>, *

2 What destinations

Destinations
app:wiki, tag:database, subnet:10.0.0.0/16, host:10.0.4.2, autogroup:internet

3 Capabilities what the source may do on the destinations

Capability 1

Protocol TCP Ports "443", "8000-8100", "22,443", "**"

Validation live, against this workspace's tags, groups, app
Fill in who, what and a capability — the controller checks it as you type.
Validate now

Preview
Who —
What —
Can tcp any port
When none

Writing a grant in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

Deny by default

A device sees nothing it has not been granted; an empty policy is no access.

Your own network per organisation

Each organisation has its own encrypted overlay; relays admit only known devices.

No inbound ports

Gateways and clients dial out; nothing on your network listens to the internet.

Humans approve elevation

Just-in-time access needs a different person's approval and expires on its own.

7 Where it fits

Retire the VPN for internal apps

Give staff access to named web apps and servers instead of a subnet.

Vendors and contractors

Time-boxed, just-in-time access to exactly one system, recorded and approved.

Secure SSH without keys

Identity-based SSH and SFTP with recordings for root and a searchable command audit.

8 Deployment and system requirements



Cloud (SaaS)

Available

Run by TotalHeal in an India region: nothing to host, updates delivered by us.



Hybrid

Partial

Available as a binary; no package or appliance image yet.



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



macOS
11 and later



Windows
10 / 11 (x64)



Linux gateway
amd64,
arm64

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

Network and access

- TotalHeal desktop app on macOS or Windows for users
- A Linux host for each gateway or connector
- Outbound HTTPS and UDP 3479 to the relay
- A Sttíz account per user

Alerts and tickets to

splunk> **Splunk**



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams



9 Technical specifications

Features	Included		
Grants, deny by default	✓ Included		
A private encrypted network per organisation	✓ Included		
Device posture	✓ Included		
Risk - adaptive access	✓ Included		
Enrolment profiles and approval	✓ Included		
Just - in - time access	✓ Included		
Gateways for private apps	✓ Included		
Secure SSH	✓ Included		
Micro - segmentation and response	✓ Included		
Availability by tier	Essential	Professional	Elite
Grants with deny by default, a private encrypted network per organisation, gateways for private apps, policy simulation	✓ Included	✓ Included	✓ Included
Enrolment profiles and approval, device posture, risk - adaptive access, quarantine and release, network map, audit log	✓ Included	✓ Included	✓ Included
Just - in - time access: request, risk analysis, human approval (never your own), time - boxed grant	—	✓ Included	✓ Included
Step - up MFA, device risk and location set by your team	—	✓ Included	✓ Included
Secure SSH and SFTP with per - session authorisation, recordings and command audit	—	—	✓ Included

Revoke a device at every gateway and restore it; audit-chain verification	—	—	✔ Included
List price per user per year	US\$72 · ₹6,850	US\$108 · ₹10,280	US\$156 · ₹14,840
Platforms and coverage			
macOS and Windows	Desktop client in the TotalHeal app (per-app mode)		
Linux (amd64, arm64)	Node for gateway roles and Secure SSH		
Controller	SaaS, India region		
Deployment options			
SaaS (controller and India relay run by TotalHeal)	Available		
Hybrid (your Linux node as router, connector or exit node)	Partial Available as a binary; no package or appliance image yet.		
On-premises controller	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	User per year		
Counted	Distinct users with an access client or session in 30 days		
Trial	30 days		
Editions	Organisations that have ZeroGate today through Enterprise or the Secure Access add-on keep every tier.		
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	TotalHeal desktop app on macOS or Windows for users
Requirement 2	A Linux host for each gateway or connector
Requirement 3	Outbound HTTPS and UDP 3479 to the relay
Requirement 4	A Sttiz account per user

10 Getting started

- TotalHeal desktop app on macOS or Windows for users
- A Linux host for each gateway or connector
- Outbound HTTPS and UDP 3479 to the relay
- A Sttiz account per 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/ztna

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.