

Network Access Control (NAC)

Only known, healthy devices on your network — and a compromised one off it in seconds

Decides which devices join your wired and wireless network and in which VLAN — by device certificate, health and policy — and moves a compromised device to quarantine the moment the SOC acts.



TotalHeal
NetworkGate

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

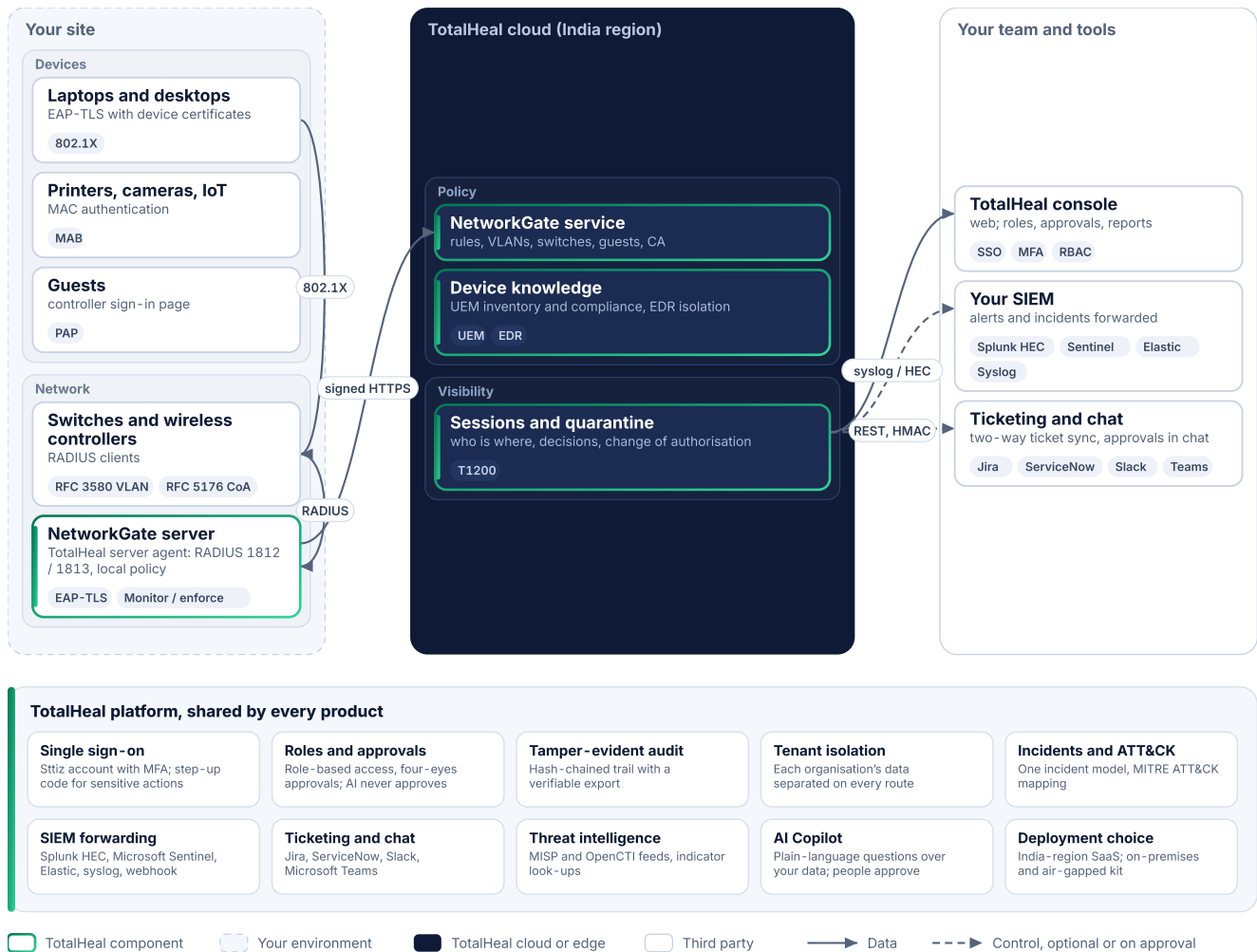
NetworkGate runs a RADIUS server of its own at each site. Switches and wireless controllers ask it about every device; it admits managed devices by certificate and UEM compliance, registered printers and cameras by MAC, guests by sponsored account, refuses the rest, and moves a device to the quarantine VLAN the moment the SOC acts.

2 The challenge

Anyone who plugs into a meeting-room port or learns the Wi-Fi password is on the same network as finance and the plant. Laptops that have stopped patching, printers and cameras that can never run an agent, contractors and guests all share it, and when a laptop is compromised the network keeps carrying its traffic until someone walks to the switch.

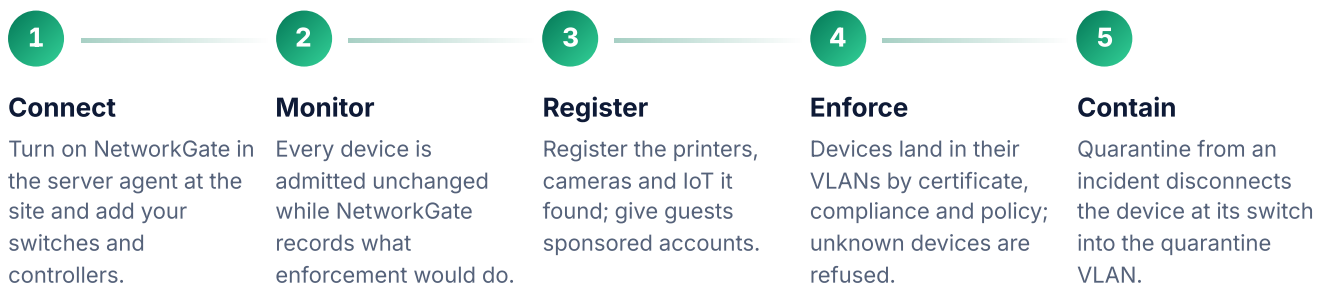
The TotalHeal approach. NetworkGate runs a RADIUS server of its own at each site in the TotalHeal server agent. Switches and wireless controllers ask it about every device: managed laptops sign in with certificates and are admitted by their UEM compliance, printers and cameras are admitted by registration, guests by sponsored accounts, and everything else is refused — with each decision, port and VLAN visible in the console. Quarantine from an incident moves the device at once.

3 Architecture

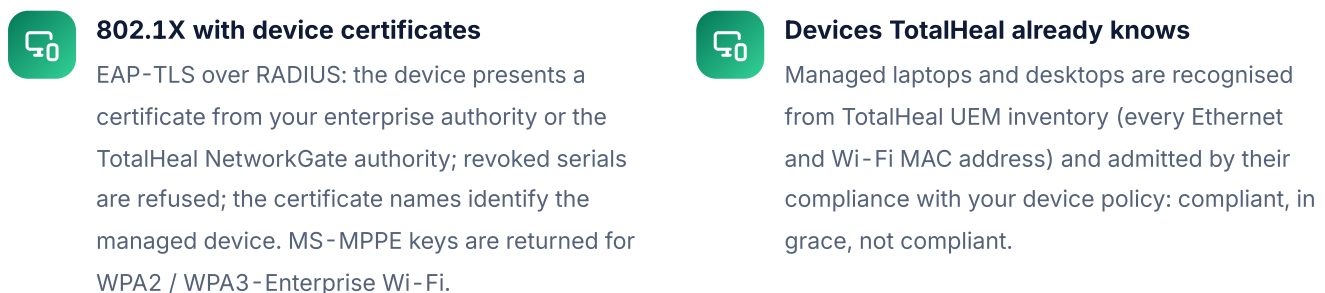


Switches ask the NetworkGate server at the site over RADIUS; the server decides from its local policy copy and reports to the cloud; quarantine reaches the switch as a change of authorisation.

4 How it works



5 Capabilities in detail





MAC authentication for what cannot do 802.1X

Printers, cameras, phones and IoT are admitted by registration (name, group, VLAN); an unknown MAC is refused and raises an alert (MITRE ATT&CK T1200 Hardware Additions).



VLANs by policy

Ordered rules over how the device signed in, what it is (managed, registered, guest, unknown), its compliance, quarantine, registered group, MAC vendor, site and SSID — allow, quarantine VLAN, guest VLAN or refuse — sent to the switch as RFC 3580 VLAN attributes. Rules are edited in the console, never as JSON.



Quarantine that takes effect now

Quarantining a device from the console or a playbook sends a RADIUS change of authorisation (RFC 5176) to the switch it is on; it re-authenticates straight into the quarantine VLAN. A device isolated by an EDR response, and optionally one with an open critical alert, is quarantined too.



Runs at your site

The RADIUS server runs in the TotalHeal server agent on a Linux server at each site, keeps its last policy on disk and keeps answering if the internet link to the cloud is down. Its EAP-TLS key never leaves it; its certificate is issued from its own signing request.



Alerts in the same incident queue

Unknown devices and quarantines join endpoint, identity and cloud alerts, and go on to your SIEM, ticketing and playbooks.



Guests

Sponsored guest accounts with an expiry for the controller's guest sign-in page (PAP); the password is shown once and stored only as a salted hash.



Monitor before you enforce

Monitor mode admits every device unchanged and records what enforcement would do, so refused devices can be registered before anyone is locked out.



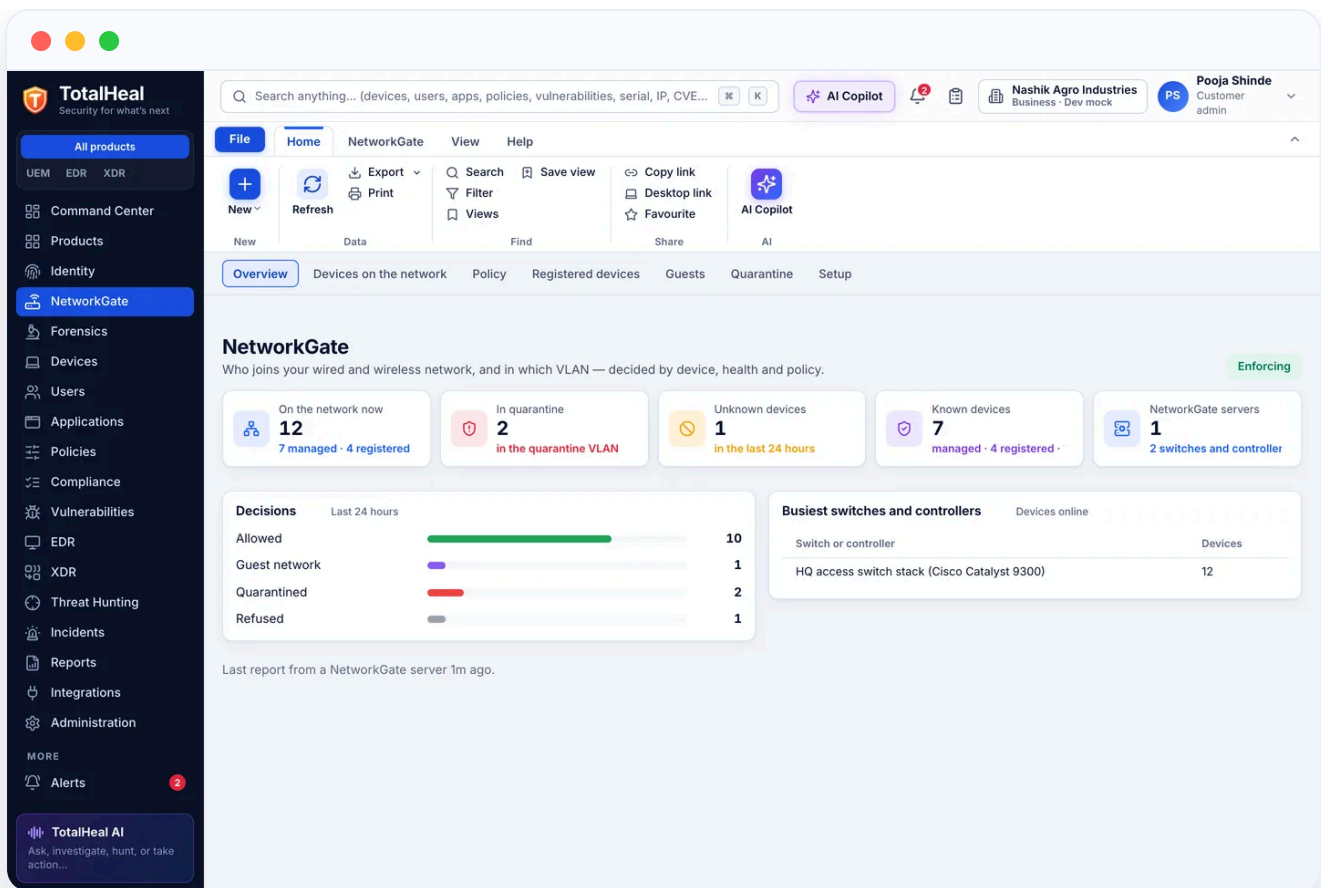
Who is where

Every device that asked: managed device or registration, switch, port, SSID, IP address from accounting, VLAN, rule and reason, online or offline, with its history of decisions and sessions.



Switch secrets handled carefully

Each switch or controller gets a generated shared secret, shown once, sealed at rest, delivered only to your NetworkGate servers and rotated in one click; requests from unknown addresses or with a wrong secret are dropped.



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

6 Security and data handling

Authentication stays local

The RADIUS server runs at your site and keeps its last policy: a cloud outage does not lock people out.

Keys stay where they belong

Each server's EAP-TLS key never leaves it; switch secrets are shown once and sealed at rest; guest passwords are kept only as hashes.

Nothing changes before you enforce

Monitor mode admits every device unchanged while showing what enforcement would do.

Every decision explained

Each device shows the rule, the reason, the switch, the port and the VLAN.

7 Where it fits

Rogue devices

A laptop or Raspberry Pi plugged into a meeting-room port is refused and raises an alert.

Patch or quarantine

Laptops that fail the device policy land in a remediation VLAN until they are compliant again.

Incident containment

The SOC moves a compromised laptop off the corporate VLAN without anyone visiting the switch.

8 Deployment and system requirements



Cloud (SaaS)

Available

Policy and visibility in the cloud; the RADIUS server at your site.



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



RADIUS switches and controllers

RFC 2865, 3580, 5176

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 Linux server at each site running the TotalHeal server agent with networkgate.enabled, reachable from the switches on UDP 1812 / 1813
- Switches and controllers configured with NetworkGate as their RADIUS server (802.1X and / or MAC authentication), and change of authorisation allowed from it
- For 802.1X: device certificates from your enterprise authority or the NetworkGate authority (UEM can deliver profiles)

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included
802.1X with device certificates	✓ Included
Devices TotalHeal already knows	✓ Included
MAC authentication for what cannot do 802.1X	✓ Included
Guests	✓ Included
VLANs by policy	✓ Included

Monitor before you enforce	✓ Included		
Quarantine that takes effect now	✓ Included		
Who is where	✓ Included		
Runs at your site	✓ Included		
Switch secrets handled carefully	✓ Included		
Alerts in the same incident queue	✓ Included		
Availability by tier	Essential	Professional	Elite
RADIUS at each site in the TotalHeal server agent; managed devices recognised from UEM inventory; MAC authentication by registration	✓ Included	✓ Included	✓ Included
VLAN policy rules, monitor mode, who-is-where sessions and events, alerts in the incident queue	✓ Included	✓ Included	✓ Included
802.1X EAP-TLS with device certificates from your authority or the NetworkGate CA	—	✓ Included	✓ Included
Sponsored guest access with expiry	—	✓ Included	✓ Included
Quarantine that takes effect now (RADIUS change of authorisation): by hand, on EDR isolation, on open critical alerts	—	—	✓ Included
List price per endpoint per year	US\$15 · ₹1,430	US\$24 · ₹2,280	US\$36 · ₹3,430
Platforms and coverage			
NetworkGate server	TotalHeal server agent on Ubuntu, Debian, RHEL, Rocky Linux or AlmaLinux at each site (networkgate.enabled); UDP 1812 / 1813		
Switches and wireless controllers	Any with RADIUS (RFC 2865 / 2866), 802.1X, MAC authentication and VLAN assignment (RFC 3580); change of authorisation needs RFC 5176 (UDP 3799)		
Devices	EAP-TLS supplicants (Windows, macOS, Linux, iOS, Android) with a device certificate; MAC authentication for printers, cameras and IoT		
Console	TotalHeal web console		

Deployment options	
SaaS (India region)	Available Policy and visibility in the cloud; the RADIUS server at your site.
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	Endpoint per year
Counted	Devices admitted to the network in the billing period
Trial	30 days, up to 50 endpoints
Editions	NetworkGate is sold on its own, outside the editions.
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	A Linux server at each site running the TotalHeal server agent with networkgate.enabled, reachable from the switches on UDP 1812 / 1813
Requirement 2	Switches and controllers configured with NetworkGate as their RADIUS server (802.1X and / or MAC authentication), and change of authorisation allowed from it
Requirement 3	For 802.1X: device certificates from your enterprise authority or the NetworkGate authority (UEM can deliver profiles)

10 Getting started

- A Linux server at each site running the TotalHeal server agent with networkgate.enabled, reachable from the switches on UDP 1812 / 1813

- Switches and controllers configured with NetworkGate as their RADIUS server (802.1X and / or MAC authentication), and change of authorisation allowed from it
- For 802.1X: device certificates from your enterprise authority or the NetworkGate authority (UEM can deliver profiles)

Start a 30 days, up to 50 endpoints 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/networkgate

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.