

IoT and unmanaged device security

Know every connected thing on your network — and keep each kind where it belongs

Finds every camera, printer, phone and building, medical or industrial device on your network, tells you what each one is and why, how risky it is, and where it may go.



TotalHeal
ThingGuard

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

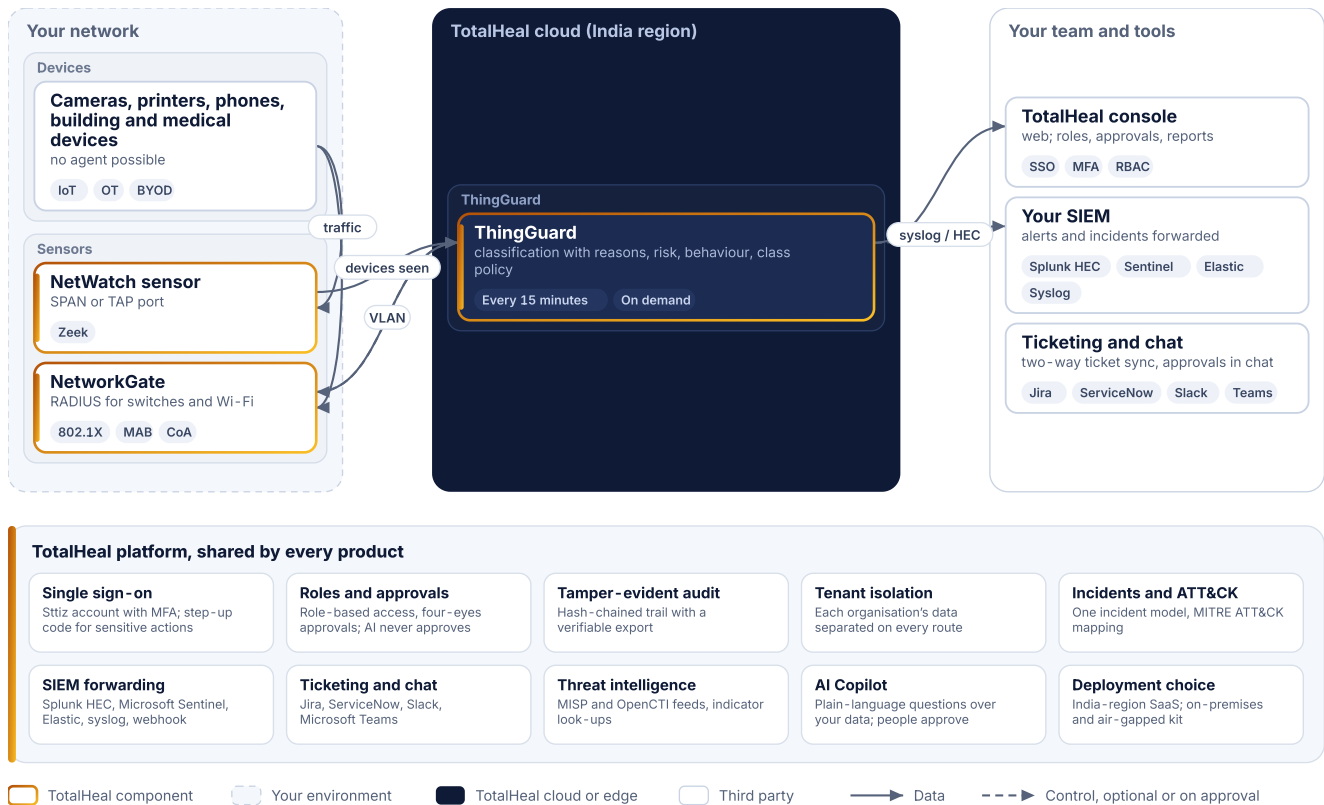
ThingGuard turns what NetWatch and NetworkGate already see into one inventory of every device, classifies each one with its reasons, scores its risk and, through NetworkGate, puts each class of device in its own VLAN or quarantine.

2 The challenge

Most of what is on a network today cannot run an agent: cameras, printers, IP phones, smart TVs, building controllers, medical modalities, sensors. Nobody has a list of them, half answer on telnet or a default web page, some are reachable from the internet through a forgotten port forward, and they sit on the same VLAN as finance — so one compromised camera is a way in for everyone.

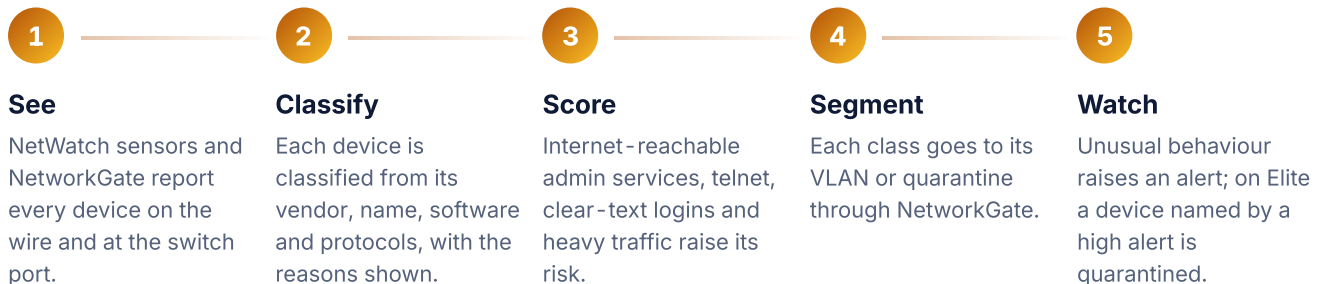
The TotalHeal approach. ThingGuard builds one inventory from what TotalHeal already sees on the wire and at the switch port — NetWatch sensors, NetworkGate sessions and UEM — and classifies every device from its manufacturer, host name, software banners and the protocols it answers on, showing the reasons. On the Professional tier it scores each device's risk, raises alerts when a device starts behaving differently and puts each class of device in its own VLAN or quarantine through NetworkGate.

3 Architecture

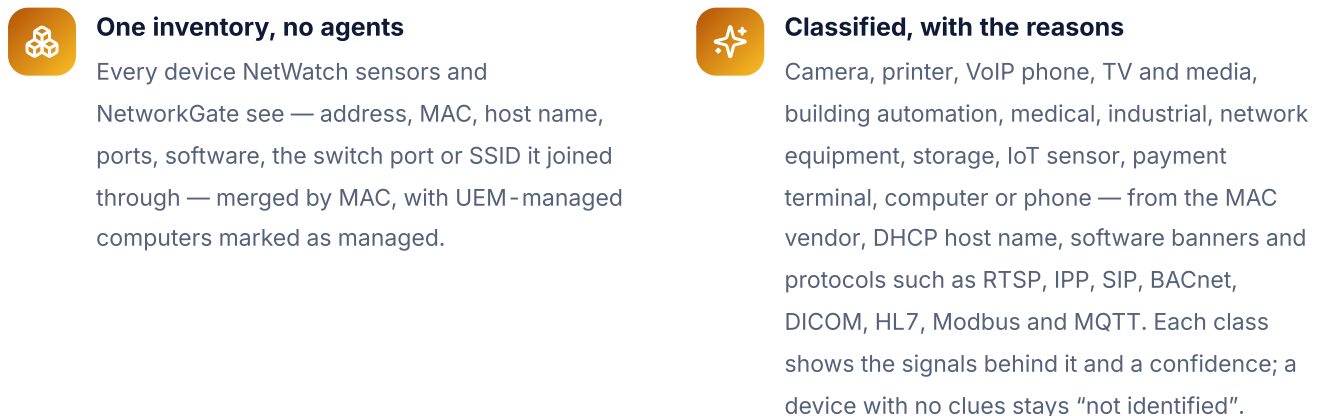


NetWatch and NetworkGate see the devices; ThingGuard classifies them, scores risk and applies the class policy back through NetworkGate.

4 How it works



5 Capabilities in detail





You can correct it

Set a device's class by hand when you know better; the next sweeps keep your choice, and the change is audited.



Behaviour alerts

A device that starts reaching dozens of new internet addresses, or whose admin service becomes reachable from the internet, raises an alert in the same incident queue as everything else (MITRE ATT&CK T1041).



Quarantine on incidents

On the Elite tier, a device named by an open high or critical alert is quarantined automatically for the classes you choose.



Risk per device

Admin services reachable from the internet, telnet and FTP, clear-text logins, web admin over plain HTTP only, heavy internet traffic and devices not registered with NetworkGate add to a 0–10 score, each factor listed.



Segmentation by class

Choose per class: leave as is, put in a VLAN, or quarantine. ThingGuard registers each device with NetworkGate in its class's VLAN or quarantines it, and switches that support change of authorisation move it at once.

The screenshot shows the TotalHeal ThingGuard interface. The left sidebar contains navigation links for various products and features. The main content area displays a table of devices under the 'Devices' tab. The table columns are: Device, Class, Vendor, Answers on, Risk, Policy, and Last seen. The data is as follows:

Device	Class	Vendor	Answers on	Risk	Policy	Last seen
lobby-cam-01 10.20.0.31 · 44:19:b6:5a:10:31	IP camera / NVR high confidence	—	23, 80, 554	High · 8	VLAN 40	3m ago
dvr-ward-b 10.20.0.33 · 3c:ef:8c:21:77:03	IP camera / NVR high confidence	—	80, 37777	Low · 1	VLAN 40	1h ago
bms-ahu-ctrl 10.20.0.70 · 00:a0:85:00:40:70	Building automation high confidence	—	80, 47808	Low · 1	—	2h ago
reception-voip 10.20.0.60 · 00:04:f2:e1:30:60	VoIP phone high confidence	—	80, 5060	Low · 1	—	2h ago
hp-laserjet-reception 10.20.0.40 · a0:d3:c1:44:90:40	Printer high confidence	—	80, 631, 9100	Low · 1	VLAN 30	2h ago
lounge-smarttv 10.20.0.80 · 8c:79:f5:12:50:80	TV and media high confidence	—	7000, 8008, 8009	Low · 0	quarantined	1h ago
parking-cam-02 10.20.0.32 · 44:19:b6:5a:10:32	IP camera / NVR high confidence	—	443, 554	Low · 0	VLAN 40	1h ago
esp-coldroom-temp 10.20.0.95 · 24:6f:28:3e:70:95	IoT sensor / gateway high confidence	—	1883	Low · 0	—	2h ago
diskstation-backup 10.20.0.90 · 00:11:32:9c:60:90	Network storage (NAS) high confidence	—	445, 5001	Low · 0	—	2h ago
10.20.0.120	Medical device	—	8888	Low · 0	VLAN 60	2h ago

ThingGuard devices for a demo diagnostics clinic, seen by a NetWatch sensor. Real screenshot, demo data.

6

Security and data handling

Reasons, not guesses

Every class shows the signals behind it; a device without clues stays not identified.

Your corrections stay

A class set by hand is kept by every later sweep.

Managed computers are left alone

Devices TotalHeal UEM manages are never moved by a class policy.

Every change is audited

Class changes, VLAN moves and quarantines are recorded with who or what made them.

7 Where it fits

Cameras on the office VLAN

Find every camera and DVR and move them to a camera VLAN without touching each switch port.

Hospitals and clinics

Know which modalities, PACS gateways and infusion devices are on the network and keep them apart.

A forgotten port forward

See the device whose telnet answers the internet before an attacker does.

8 Deployment and system requirements



Cloud (SaaS)

Available

Classification and policy run in the TotalHeal cloud; sensors and NetworkGate stay on your network.



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



Any IP device on a monitored network
seen by NetWatch or NetworkGate



RADIUS switches and controllers
VLANs and quarantine through NetworkGate

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 TotalHeal NetWatch sensor on a SPAN or TAP port, or NetworkGate on your switches
- NetworkGate for VLANs and quarantine by class

Alerts and tickets to

splunk> Splunk

Microsoft Sentinel

Elastic

Syslog / CEF

Jira

ServiceNow

Slack

Microsoft Teams

Features	Included		
One inventory, no agents	✓ Included		
Classified, with the reasons	✓ Included		
You can correct it	✓ Included		
Risk per device	✓ Included		
Behaviour alerts	✓ Included		
Segmentation by class	✓ Included		
Quarantine on incidents	✓ Included		
Availability by tier	Essential	Professional	Elite
One device inventory from NetWatch, NetworkGate and UEM: address, MAC, host name, ports, software, switch port or SSID	✓ Included	✓ Included	✓ Included
Each device classified (camera, printer, VoIP phone, TV, building, medical, industrial, network, storage, IoT sensor, payment terminal, computer, phone) with its reasons and confidence; class set by hand when you know better	✓ Included	✓ Included	✓ Included
Risk per device: admin services reachable from the internet, telnet and FTP, clear-text logins, plain-HTTP admin, heavy internet traffic, unregistered on NetworkGate	—	✓ Included	✓ Included
Alerts when a device starts reaching many new internet addresses or exposes an admin service	—	✓ Included	✓ Included
A VLAN or quarantine per device class, applied through NetworkGate as devices are seen	—	✓ Included	✓ Included
Automatic quarantine of a device named by a high or critical alert	—	—	✓ Included

List price per device per year	US\$9 · ₹860	US\$18 · ₹1,710	US\$27 · ₹2,570
Platforms and coverage			
Discovery	TotalHeal NetWatch sensor (Zeek) on a SPAN or TAP port; NetworkGate RADIUS sessions; TotalHeal UEM inventory		
Segmentation	Through NetworkGate: switches and wireless controllers speaking RADIUS (RFC 2865, 3580; change of authorisation RFC 5176)		
Console	TotalHeal web console		
Deployment options			
SaaS (India region)	Available Classification and policy run in the TotalHeal cloud; sensors and NetworkGate stay on your network.		
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	device per year		
Counted	Devices in the ThingGuard inventory		
Trial	30 days, up to 100 devices		
Editions	ThingGuard is sold on its own, outside the editions. VLANs and quarantine need NetworkGate.		
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 TotalHeal NetWatch sensor on a SPAN or TAP port, or NetworkGate on your switches
Requirement 2	NetworkGate for VLANs and quarantine by class

10 Getting started

- A TotalHeal NetWatch sensor on a SPAN or TAP port, or NetworkGate on your switches
- NetworkGate for VLANs and quarantine by class

Start a 30 days, up to 100 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/thingguard

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.