

Network Detection & Response (NDR)

Detecting what agents cannot see, from the network itself

Network detection and response from a passive sensor: beaconing, DNS tunnelling, data leaving, lateral movement and exposed services — no agent on the hosts.



TotalHeal
NetWatch

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

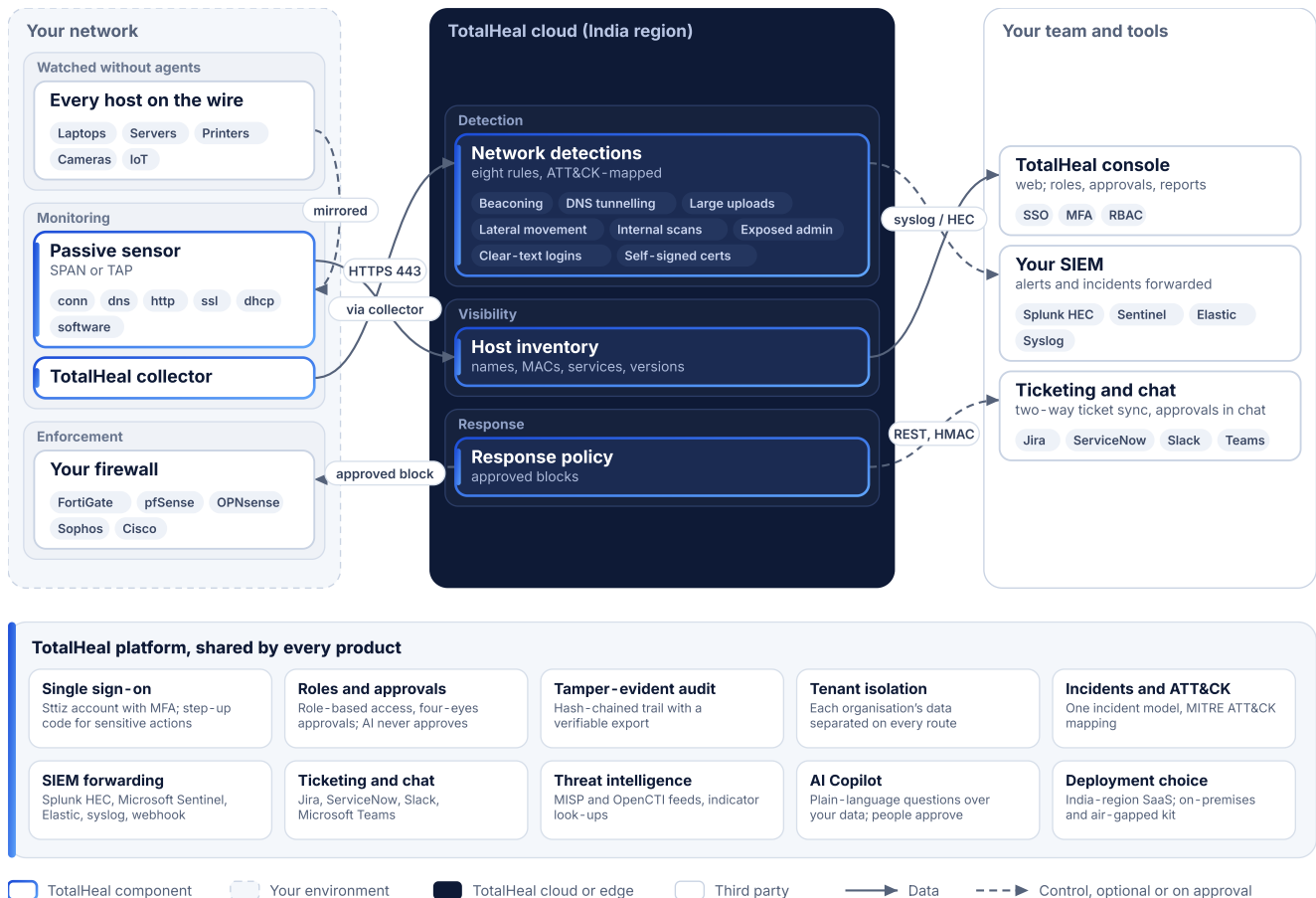
NetWatch reads connection metadata from a passive sensor and detects beaconing, DNS tunnelling, large uploads, lateral movement and exposed services — for every device on the wire, including the ones that can never run an agent.

2 The challenge

Printers, cameras, appliances and unmanaged laptops cannot run an agent, and attackers know it. What they do still crosses the network: implants call home on a timer, data leaves in large uploads, and admin protocols move from host to host.

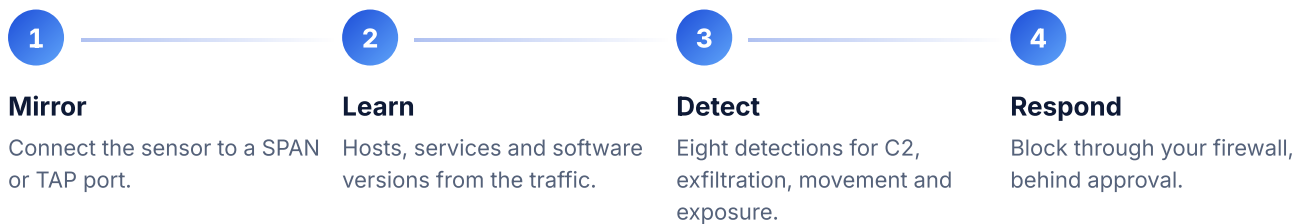
The TotalHeal approach. NetWatch runs on the same passive sensor as IndustrialGuard. It reads connection metadata from a SPAN or TAP port, detects command-and-control, exfiltration and lateral movement, learns a host inventory from the traffic and raises alerts in the same incidents as your endpoint, identity and cloud alerts.

3 Architecture

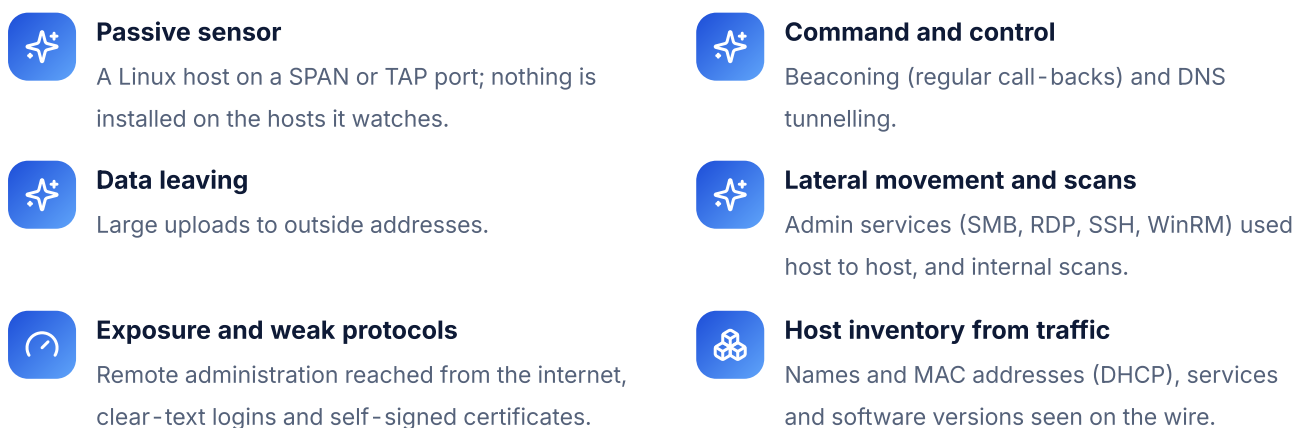


The sensor reads mirrored traffic metadata; detections join the same incidents as endpoint, identity and cloud alerts; blocks go through your firewall.

4 How it works



5 Capabilities in detail





Response through your firewall

Blocking goes through the TotalHeal firewall connectors, behind your response policy.

6 Security and data handling

Passive

Nothing is installed on watched hosts.

People approve blocks

Blocking follows your response policy.

Metadata, not content

Encrypted content is not inspected or stored.

7 Where it fits

Unmanaged devices

Cameras and printers calling home.

Data theft

Large uploads to outside addresses.

Ransomware staging

Lateral movement on admin protocols.

8 Deployment and system requirements



Cloud (SaaS)

Available

Events go through the TotalHeal collector.



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

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 host with a SPAN or TAP port
- The TotalHeal collector

Alerts and tickets to

splunk>

Splunk



**Microsoft
Sentinel**



Elastic



**Syslog /
CEF**



Jira



ServiceNow



Slack



**Microsoft
Teams**



9 Technical specifications

Features	Included	
Passive sensor	✔ Included	
Command and control	✔ Included	
Data leaving	✔ Included	
Lateral movement and scans	✔ Included	
Exposure and weak protocols	✔ Included	
Host inventory from traffic	✔ Included	
Response through your firewall	✔ Included	
Availability by edition	Business	Enterprise
Passive sensor, eight network detections, host inventory, alerts in incidents	✔ Included	✔ Included
Platforms and coverage		
Sensor	Ubuntu, Debian, RHEL -family Linux with a SPAN or TAP port	
Console	TotalHeal web console	
Deployment options		
Sensor at your site, SaaS console (India region)	✔ Available Events go through the TotalHeal collector.	
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	Sensor per year	
Counted	Sensors sending to the organisation	
Trial	30 days	
Editions	NetWatch is sold on its own, outside the editions.	
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 Linux host with a SPAN or TAP port
Requirement 2	The TotalHeal collector

10 Getting started

- A Linux host with a SPAN or TAP port
- The TotalHeal collector

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/netwatch

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.