

OT & Industrial Security

Seeing the plant network without touching it

A passive OT sensor: industrial protocols, an asset inventory learned from them, and detections for PLC stop, program download and firmware changes.



TotalHeal
IndustrialGuard

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

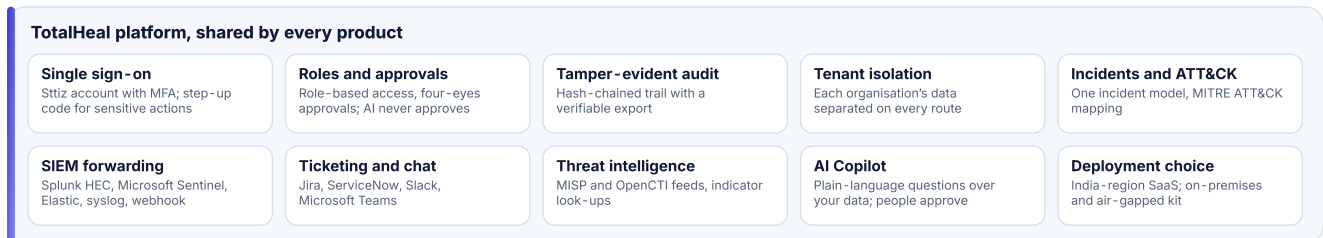
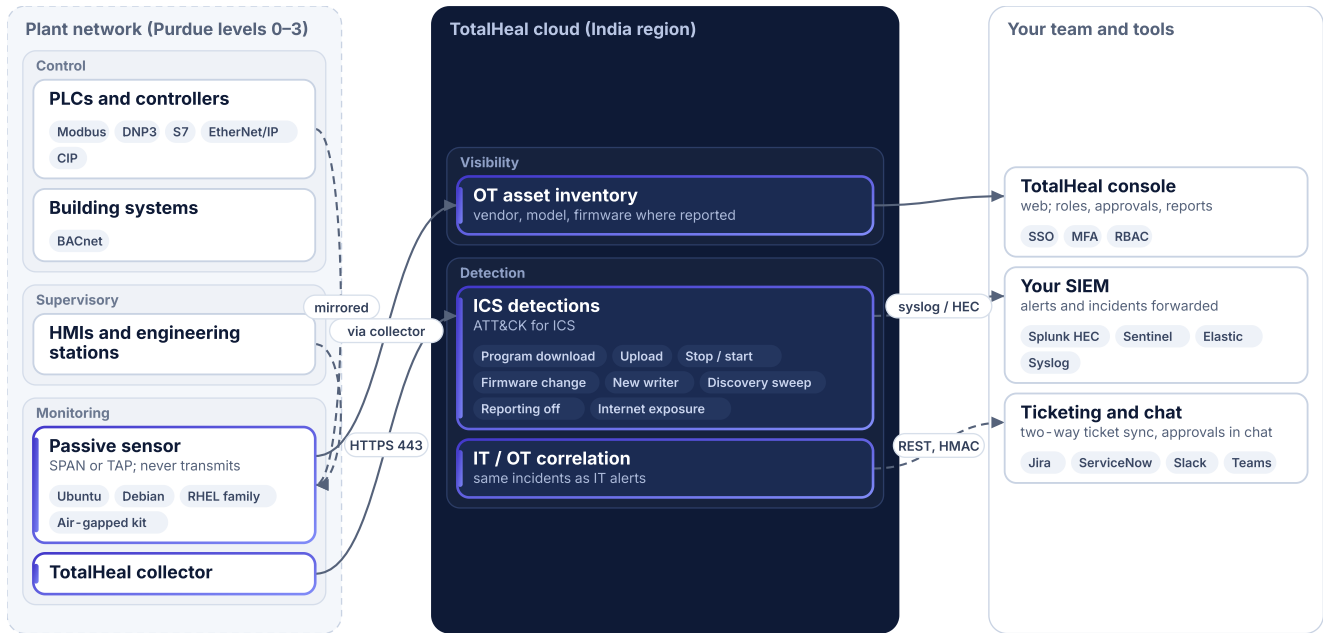
IndustrialGuard listens passively on a SPAN or TAP port, parses industrial protocols, builds an asset inventory from what controllers report and detects program downloads, controller stops and firmware changes — mapped to ATT&CK for ICS and raised next to IT alerts.

2 The challenge

Control networks run PLCs, HMIs and engineering stations that cannot take an agent and must never be scanned. Plant teams often do not know every controller on the network, and nobody would notice a program download at 2 a.m.

The TotalHeal approach. IndustrialGuard listens on a SPAN or TAP port and never sends a packet to the plant network. It parses industrial protocols, builds the asset inventory from what the devices say, and raises ICS-specific detections next to your IT alerts.

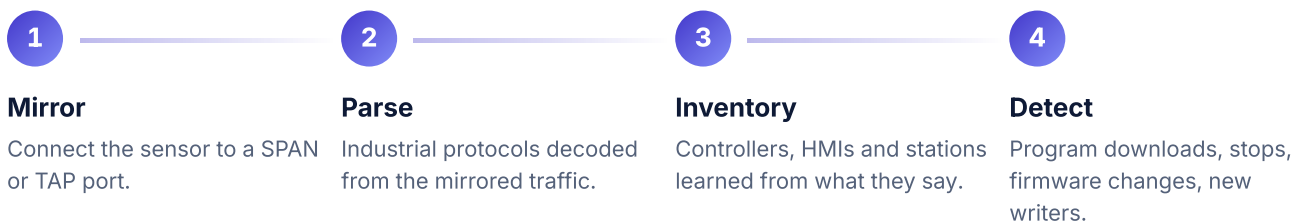
3 Architecture



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

The sensor only listens on a SPAN or TAP port; events reach the TotalHeal cloud through the collector; nothing is installed on controllers.

4 How it works



5 Capabilities in detail

- Strictly passive**
 The sensor listens on a SPAN or TAP port and never transmits on the control network.
- Industrial protocols**
 Modbus, DNP3, Siemens S7, EtherNet/IP and CIP, and BACnet parsed, using the open CISA ICS protocol parsers.



Asset inventory

Controllers, engineering stations and HMIs, with vendor, model and firmware where the protocol reports them.



ICS detections

Program download and upload, controller stop and start, firmware change, new writers to a controller, discovery sweeps, reporting disabled and internet exposure — mapped to MITRE ATT&CK for ICS.



One place for IT and OT

OT alerts arrive in the same console and incidents as endpoint, network and identity alerts.



Air-gapped install

The sensor installs online or from an offline kit on Ubuntu, Debian and RHEL -family Linux.

6 Security and data handling

Never transmits

The sensor never sends a packet to the plant network.

No agents on controllers

Nothing is installed on OT devices.

Offline install

Installs from an air-gapped kit.

7 Where it fits

Unknown controllers

A first inventory of the plant network.

Change detection

Program downloads outside maintenance windows.

IT/OT incidents

An IT compromise reaching OT in one incident.

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



Modbus · DNP3 · S7



EtherNet/IP · CIP · BACnet

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

Network and access

- A Linux host with a SPAN or TAP port on the control network
- The TotalHeal collector

Alerts and tickets to

splunk> Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

Sign-in

Active Directory / LDAP, SAML 2.0
or OpenID Connect

Software

Nothing to pre-install: no
container runtime, database, web
server or Java



9 Technical specifications

Features		Included
Strictly passive	✓	Included
Industrial protocols	✓	Included
Asset inventory	✓	Included
ICS detections	✓	Included
One place for IT and OT	✓	Included
Air-gapped install	✓	Included
Availability by edition		BusinessEnterprise
Passive sensor, protocols, asset inventory, ICS detections	✓	IncludedIncluded
Platforms and coverage		
Sensor	Ubuntu, Debian, RHEL -family Linux with a SPAN or TAP port	
Protocols	Modbus, DNP3, S7, EtherNet/IP / CIP, BACnet	
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	No Business/Enterprise split is set for IndustrialGuard yet.
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 on the control network
Requirement 2	The TotalHeal collector

10 Getting started

- A Linux host with a SPAN or TAP port on the control network
- 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/ot-security

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.