DEEP PROTOCOL & ASSET INTELLIGENCE

Your network is already telling you what every device is. We listen properly.

Every device on a network announces itself continuously. It negotiates certificates, answers discovery requests, identifies its vendor and firmware, and issues commands that describe exactly what it does for a living. That information is already crossing the wire, in the clear, every second of every day.

Most security tools skim it. They record that two addresses exchanged traffic on a port and move on. WireTrace reads what was actually said, and turns it into an inventory you can trust, exposure you can act on, and evidence you can hand to an auditor.

250+	4	0	Minutes
PROTOCOLS READ IN DEPTH	DOMAINS ON ONE PLATFORM	AGENTS, PROBES OR SCANS	FROM CONNECTION TO FIRST ASSETS

THE PROBLEM WORTH SOLVING

The devices that carry the most risk are the ones your existing tools cannot reach. A protection relay will not run an agent. An infusion pump will not accept one. A twelve-year-old PLC running a production line will fault if you scan it, and the plant manager is right to refuse. So the estate splits in two: the part that is managed and visible, and the part that is neither, which is usually where an incident starts.

Asking those devices what they are is the wrong move, and in safety-critical environments it is a dangerous one. **They are already saying it.** The question is whether anything on the network is listening closely enough to understand.

WHAT WIRETRACE DOES

WireTrace connects to a SPAN port or a network TAP and observes. It transmits nothing onto the monitored network, installs nothing on any device, and asks no device any question. From that vantage point it reads protocol conversations in depth and builds a continuously updated picture of the environment: what each device is, who made it, what firmware it runs, what it talks to, what it is being told to do, and whether any of that has changed.

A live asset inventory, derived not entered
Vendor, model, role, firmware and identity established from what devices say on the wire, including the unmanaged and undocumented ones nobody put in the CMDB.

Communication relationships as they really are
Which device actually talks to which, over what protocol, in which direction. The map of the network as it behaves, rather than as the design document claims.

Exposure grounded in observation
Cleartext credentials, weak certificates, exposed management paths and unprotected industrial protocols, found because they were seen, not because a scanner guessed.

Compliance evidence from real traffic
Control evidence assembled continuously from observed communications, so an audit becomes a report to review rather than a project to staff.

FOUR DOMAINS, ONE PLATFORM

OT
PLCs, RTUs, drives, protection relays, historians and engineering workstations, watched without touching the process.

IT
Servers, endpoints, network infrastructure and the shadow systems that never made it onto anyone's list.

IoT
Cameras, access control, building management, printers and the long tail of connected equipment nobody owns.

IoMT
Infusion pumps, imaging systems, patient monitors and diagnostics, where a scan is a clinical risk.

WHAT THAT MAKES POSSIBLE

The value of reading protocols properly shows up in questions that are normally hard to answer, and that WireTrace answers from traffic alone.

WITHOUT TOUCHING IT

Identify a device down to its firmware

Make, model and firmware version established from how a device identifies itself in its own protocols, on equipment that would fault under a scan and will never run an agent.

BEYOND OPEN PORTS

See what a controller is actually being told to do

Not that a port is open, but which commands are being issued, to which device, by whom, and whether that pattern is what it was yesterday.

DESIGN VERSUS REALITY

Prove segmentation is holding

Zones are enforced on paper and eroded in practice. Observed traffic shows which boundaries are real and which have quietly been crossed.

EVIDENCE, NOT INTERVIEWS

Answer an auditor from communications

Control evidence drawn from what the network actually did during the assessment window, with the observation behind every statement.

NOTHING LEAVES

Investigate with AI inside an air-gapped network

Rumi, the WireTrace assistant, runs entirely within the customer environment. No cloud service, no external call, no data leaving the boundary.

THE UNKNOWN ESTATE

Find the devices nobody documented

Contractor equipment, forgotten test rigs, replaced hardware still connected. If it speaks on the network, it appears in the inventory.

BUILT FOR THE ENVIRONMENTS THAT MAKE THIS HARD

Passive by architecture, not by setting

There is no active mode to leave switched on by accident. WireTrace observes; it does not interrogate. That is what makes it safe on a production line and on a clinical network.

On premises and sovereign

Fully self-contained. No cloud dependency and no data leaving the network, which is what regulated, national and defence environments require before a conversation can even start.

Air-gap capable

Designed to run in isolated networks with no outbound path, including the analytics and the AI assistant. Isolation does not have to mean going without modern tooling.

Value in minutes

Connect to a SPAN port or TAP and assets begin appearing and classifying within minutes. No agent rollout, no scan window, no change freeze to negotiate.

WHERE IT EARNS ITS PLACE

YOU NEED TO	WIRETRACE GIVES YOU
Know what is on the network	A live inventory built from observed behaviour, including everything agents and scanners cannot reach.
Reduce real exposure	Weaknesses that were observed in traffic, prioritised by what is actually reachable and actually running.
Satisfy a regulator	Continuous control evidence drawn from communications, mapped to the frameworks you are assessed against.
Detect what does not belong	Changes in device behaviour and communication relationships, with the protocol context needed to judge them.
Understand your estate physically	Where devices actually sit, how they are connected, and what a path between two of them really traverses.

See it against your own traffic

The fastest way to judge WireTrace is to point it at a live segment of your network and look at what comes back within the hour. We will show you the inventory it builds, the exposure it finds, and the evidence it produces, using your environment rather than a demonstration dataset.

Book a demo at wiretrace.io/request-demo · or email sales@wiretrace.io