DEEP PROTOCOL & ASSET INTELLIGENCE

# Complete visibility of every device on the network, without touching a single one of them.

WireTrace observes network traffic passively and reads protocol conversations in depth to produce a continuously updated asset inventory, real exposure, behavioural context and audit evidence across operational technology, enterprise IT, connected devices and medical equipment. No agents. No active scanning. No cloud dependency.

| 250+ | 4 | Minutes | 100% |
|---|---|---|---|
| PROTOCOLS READ IN DEPTH | DOMAINS, ONE PLATFORM | TO FIRST CLASSIFIED ASSETS | PASSIVE, ON PREMISES |

## WHAT WIRETRACE DISCOVERS

- ✓ **Device identity.** Vendor, model, role and firmware, derived from observed protocol behaviour.
- ✓ **Communication relationships.** Who talks to whom, over what, in which direction.
- ✓ **Network structure.** How the estate is physically and logically put together.
- ✓ **Unmanaged assets.** Equipment no agent reaches and no inventory records.
- ✓ **Protocol behaviour.** The commands, values and identifiers exchanged, not just the session.
- ✓ **Change.** New devices, new relationships and new behaviour, as they appear.

## WHAT WIRETRACE PRODUCES

### Asset inventory
A live record of every device observed, with identity, role, protocols spoken, peers and history. Built from behaviour, so it stays accurate without manual maintenance.

### Exposure and vulnerability context
Security-relevant conditions observed directly in traffic, and vulnerability correlation driven by observed firmware and real reachability so that prioritisation reflects the estate rather than a generic severity score.

### Security findings with protocol context
Behavioural change, unexpected relationships and indicators matched against threat intelligence, each presented with the protocol detail an analyst needs to make a judgement.

### Compliance evidence
Control evidence assembled continuously from observed communications and mapped to the frameworks you are assessed against, with source observations retained.

### Physical and logical topology
Where devices sit, how they connect, and what a communication path between any two of them actually traverses, including a three-dimensional model of the environment.

### Private AI investigation
Rumi answers questions about your environment using your own observed data, running entirely inside your network including air-gapped deployments.

## DOMAIN COVERAGE

### OT
Process control, energy and manufacturing systems, observed without interacting with the process.

### IT
Servers, endpoints, infrastructure and the shadow systems outside the managed estate.

### IoT
Cameras, access control, building management and connected equipment across the facility.

### IoMT
Clinical and diagnostic devices, where active interrogation is a patient safety concern.

## PROTOCOL ANALYSIS

**Industrial control**
Process, energy, manufacturing and safety protocols, read for the commands and values they carry.

**Medical**
Clinical imaging and messaging exchanges including DICOM and HL7, handled to suit a patient environment.

**Enterprise**
Directory, transport, web, file, mail and remote access, including security-relevant detail.

**Infrastructure**
Discovery, management, routing and building systems that describe the network itself.

More than 250 protocols are analysed for their content and meaning rather than classified by port. Coverage detail for a specific protocol, including what is and is not recoverable from it, is available on request as part of a technical evaluation.

## DEPLOYMENT

| ASPECT | DETAIL |
|---|---|
| **Network connection** | SPAN port or network TAP. Nothing is transmitted onto the monitored network. |
| **Endpoint footprint** | None. No agents, no software installed on any observed device. |
| **Time to value** | Assets begin appearing and classifying within minutes of connection. |
| **Hosting** | Fully on premises. No cloud dependency and no data leaving the network. |
| **Isolated networks** | Air-gap capable, including analytics and the AI assistant. |
| **Scale** | Multiple sensors report to a central platform for distributed and multi-site estates. |
| **Access control** | Role-based access with multi-tenant separation for grouped or managed environments. |
| **Integration** | Findings, inventory and evidence are available to existing security and operations tooling. |

## COMPLIANCE FRAMEWORKS

Evidence is mapped across **seven frameworks and 415 controls**: **NIST CSF 2.0**, **ISO 27001**, **HIPAA Security Rule**, **IEC 62443-3-3**, **NERC CIP**, **NCA OTCC** and **NCA ECC**. Every control carries its own rating for how far network observation can take it, from fully observable through to not assessable, so an assessment starts from an accurate position rather than an optimistic one.

## WHY ORGANISATIONS CHOOSE WIRETRACE

**Safe in environments that forbid scanning**
Passive by architecture rather than by configuration. There is no active mode to enable by mistake on a production line or a clinical network.

**One platform across four domains**
The same sensor and the same platform cover industrial, enterprise, connected and medical devices, without per-domain modules or separate tools to reconcile.

**Sovereign and self-contained**
Nothing depends on a vendor cloud. Suitable for regulated, national and defence environments where data residency is a precondition.

**Evidence that survives the meeting**
Findings retain the observations behind them, so they can be defended to an engineer, an auditor or an investigator later.

### Evaluate it against your own network

A scoped evaluation connects WireTrace to a representative segment and reports what it found: the inventory, the exposure, and the evidence, from your traffic rather than a prepared dataset. Most of the interesting findings appear on the first day.

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