

SOLUTION BRIEF

The plant will not let you scan it,  
and it is right not to.

Operational networks are full of equipment that predates the idea of being interrogated. A protection relay, a twenty-year-old controller, a safety system on a certified configuration: each will refuse an agent, and some will fault or drop into a safe state if probed. Operations knows this, which is why the answer to a scanning request is usually no, and why it should be.

So the plant stays invisible to security tooling, and the security programme reports on the corporate network while the part that can actually hurt someone remains a list in a spreadsheet from the last integration project.

WHAT MAKES THIS ENVIRONMENT DIFFERENT

Availability outranks everything

A false positive on a corporate network is an annoyance. An intervention on a running process is a production stoppage or a safety event, so the tolerance for anything active is close to zero and will not move.

The equipment outlives the security model

Controllers installed under a different threat model are still running the process. They cannot be patched on a normal cycle, cannot host software, and will be there long after the current programme is over.

Vendor and integrator access is real and undocumented

Remote support paths are agreed commercially and rarely recorded in a network diagram. They are frequently the most privileged route into the process and the least monitored.

Segmentation drifts quietly

Zone boundaries are designed properly and then eroded by a temporary rule, a shared historian or a maintenance laptop that never left. Nothing announces the erosion.

WHAT WIRETRACE DOES HERE

WireTrace connects to a SPAN port or TAP and observes. It transmits nothing onto the process network and installs nothing on any controller. From the traffic alone it identifies what is present, what each device is, what it is being told to do, and whether that has changed.

| QUESTION                          | ANSWERED FROM OBSERVED TRAFFIC                                                                                                                 |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| What is actually on this network? | Controllers, drives, relays, historians, engineering workstations and the equipment nobody recorded, identified by vendor, model and firmware. |
| Who is issuing control commands?  | Which initiators write to which devices, using which functions, and whether that relationship existed last week.                               |
| Is the zone boundary holding?     | The traffic that actually crosses between levels, compared against what the design says should cross.                                          |
| Where is the process exposed?     | Unauthenticated control protocols, cleartext credentials, management interfaces reachable from the wrong side of a boundary.                   |
| What changed after the shutdown?  | New devices, new relationships and new command patterns that appeared during maintenance and were never removed.                               |

PROTOCOL DEPTH WHERE IT MATTERS

Industrial protocols are read for the commands and values they carry rather than counted as sessions. Coverage includes **Modbus**, **DNP3**, **IEC 61850** including **GOOSE**, **IEC 60870**, **S7**, **EtherNet/IP** and **CIP**, **PROFINET**, **OPC**, **BACnet** for facility systems, and the broader set of more than 250 protocols across the estate. The difference is between knowing that port 502 is open and knowing which function is being called against which register range, by whom.

## WHERE IT IS USED

## USE CASE

**Establishing the first real asset inventory**

Most sites have a list assembled during commissioning and amended by memory. Observation replaces it with a live record that includes the equipment added by three integrators over ten years.

## USE CASE

**Validating segmentation before an audit**

Zone and conduit design is assessed against what actually crosses the boundary, which is the evidence an assessor asks for and the one most sites cannot produce.

## USE CASE

**Watching vendor remote access**

Support sessions into the process become visible: who connected, to what, over which protocol, and what was issued while they were there.

## USE CASE

**Prioritising vulnerabilities that are real**

Correlation driven by observed firmware and actual reachability, so the remediation conversation with operations is about a short defensible list rather than a scanner export.

## USE CASE

**Detecting change in a stable process**

Process networks are repetitive, which makes deviation meaningful. A new initiator or an unfamiliar command pattern stands out in a way it never would on a corporate network.

## USE CASE

**Bridging the IT and OT reporting gap**

One platform covering both sides means the board sees a single position rather than two reports that cannot be reconciled.

## REGULATORY CONTEXT

Evidence is generated continuously from observed communications and mapped to the frameworks industrial operators are assessed against, including **IEC 62443-3-3**, **NERC CIP** for bulk electric system operators, **NIST CSF 2.0** and, for operators in the Kingdom of Saudi Arabia, the **NCA OTCC** and **NCA ECC** controls. Each mapping is explicit about what can be evidenced from network observation and what cannot, so an assessment begins from an accurate position rather than an optimistic one.

**The conversation with operations is short.** Nothing is installed on any device, nothing is transmitted onto the process network, and a sensor that fails simply stops producing observations. The objection that stops most security tooling at the plant boundary does not apply, which is usually the reason WireTrace gets approved where other approaches did not.

## DEPLOYMENT SHAPE

**Single plant**

Sensors at the points where the process aggregates, reporting to a platform on site.

**Multi-site operator**

Sensors across generating stations, substations or plants, with one estate-wide picture centrally.

**Isolated networks**

Full capability inside an air-gapped environment, including analytics and the AI assistant.

**Start with one cell, one line or one substation**

A scoped assessment needs a mirror port and a short observation window. It returns what is genuinely present on that segment, what is exposed, and what evidence can be produced. Operations can watch it happen and confirm for themselves that nothing was transmitted.

[Book a demo at wiretrace.io/request-demo](https://wiretrace.io/request-demo) · or email [sales@wiretrace.io](mailto:sales@wiretrace.io)