

IDENTIFY WITHOUT TOUCHING

Know a device's make, model and firmware without ever contacting it.

The conventional way to identify a device is to ask it, either through an agent installed on it or a scanner interrogating it. Both are unavailable on the equipment where identification matters most.

THE SITUATION

A plant, a hospital or a campus contains equipment that cannot host software and must not be probed. That equipment is nonetheless the part of the estate carrying old firmware, default configurations and known vulnerabilities. Identification is exactly what is needed and exactly what conventional tooling cannot obtain.

WHAT IS ACTUALLY AVAILABLE

Devices identify themselves constantly as a side effect of working. They announce themselves to management systems, describe their capabilities during negotiation, present certificates carrying organisational detail, respond to discovery from peers and reveal vendor and model characteristics in how they use their own protocols. None of it is hidden, and none of it requires a question.

WHAT WIRETRACE DOES

Identity is assembled from everything a device reveals across every protocol it speaks, not from a single indicator. The output is a device record with a **vendor**, a **model**, a **role** and a **firmware version**, produced entirely from observation.

Why it matters. Firmware version is the input that makes vulnerability work meaningful. Without it, exposure management on unmanaged equipment is guesswork built on a device type. With it, the conversation with the operations team is about a specific device running a specific version, which is a conversation that can actually end in a decision.

WHERE THIS SHOWS UP

Industrial

A relay or controller that will fault under a scan and has run the same firmware for a decade.

Healthcare

A pump or monitor on a validated configuration that cannot be modified without revalidation.

Enterprise

Appliance-class equipment with no supported way to install anything, holding credentials.

HOW TO TEST THIS

ASK ANY VENDOR

Show me the make, model and firmware of a device on my network that you have never seen before, without touching it.

WHAT WE WOULD SHOW YOU

Identification built from observation alone, on a device you nominate, including one your current tooling lists only as an address.

BEYOND OPEN PORTS

See what a controller is being told to do, not just that something is talking to it.

Knowing that a port is open is a statement about configuration. Knowing which commands are crossing it is a statement about what is happening to your process.

THE SITUATION

Industrial protocols carry instructions. A device is told to read a value, write a value, change a mode or transfer a program. Tools that stop at protocol identification see a session on a port and record its size and duration. That record cannot distinguish a routine poll from a configuration change.

WHAT WIRETRACE DOES

Industrial protocol conversations are read for the operations they carry: **which function is being invoked, against which device, by which initiator, and against which part of that device's address space**. The commands become part of the device's behavioural record rather than an opaque byte count.

BECOMES VISIBLE

Who is allowed to write

Most devices in a process are read by many systems and written by very few. That asymmetry is a strong control statement, and it is only visible if commands are understood.

BECOMES VISIBLE

Change outside the change process

A configuration change or program transfer that did not correspond to a raised change is one of the highest-value findings available in an operational network.

Why it matters. In a process network, an attacker who has reached the point of issuing control commands has reached the point where physical consequences begin. Detection that operates at the level of sessions and volumes cannot see that moment. Detection that understands commands can.

WHERE THIS SHOWS UP

Process control

Distinguishing a routine poll from a configuration change on a running line.

Energy

Command activity against protection and control equipment across a substation estate.

Change assurance

Program transfers and mode changes that never appeared in a change record.

HOW TO TEST THIS

ASK ANY VENDOR

For an industrial protocol I care about, what do you extract beyond the fact that a session occurred?

WHAT WE WOULD SHOW YOU

The operations actually being carried on that protocol on a live segment: which function, which initiator, which part of the device.

DESIGN VERSUS REALITY

Prove your segmentation is holding, rather than assuming it from the config.

Segmentation is designed carefully, implemented correctly, and then eroded gradually by individually reasonable exceptions. Nothing announces the erosion, and the configuration still looks right.

THE SITUATION

A firewall configuration describes what is permitted. It does not describe what occurred. Between the two sit temporary rules that became permanent, dual-homed systems nobody classified, shared services reachable from both sides, and maintenance equipment that was connected once and never removed. Every one of those is invisible in a configuration review.

WHAT WIRETRACE DOES

Observed traffic shows **what actually crossed each boundary**, in which direction, over which protocol and between which identified devices. Comparing that against the intended design converts a segmentation question from an argument into a factual matter.

BEFORE**A design review**

Rule sets are examined and declared consistent with the zone model. The review cannot detect a path that exists through a device rather than through a rule.

AFTER**An observation**

Every crossing that occurred during the window is listed, with the devices at both ends identified. The exceptions are named rather than suspected.

Why it matters. Segmentation is the control most organisations rely on most heavily and verify least directly. It is also the control an assessor probes hardest, because everyone claims it and few can demonstrate it. Observation is the demonstration.

WHERE THIS SHOWS UP

IT to OT

The seam where a corporate foothold becomes a process consequence.

Clinical

Separating patient-connected equipment from general hospital traffic, and proving it.

Audit

The control an assessor probes hardest because everyone claims it and few can show it.

HOW TO TEST THIS

ASK ANY VENDOR

How do you demonstrate that a boundary held, rather than that a rule permitting it exists?

WHAT WE WOULD SHOW YOU

Every crossing observed during the window, with the device at each end identified, set against the boundary as designed.

EVIDENCE, NOT INTERVIEWS

Answer an auditor from what the network actually did.

The weakest moment in any assessment is the follow-up question. Not "do you have a control", but "how do you know it was operating". Documents rarely survive it.

THE SITUATION

Compliance evidence is typically assembled shortly before an assessment, from policies, screenshots, exports and conversations. It describes intent accurately and operation only indirectly, and it goes out of date the moment it is collected. Producing it consumes weeks of skilled attention every cycle.

WHAT WIRETRACE DOES

Control evidence is drawn continuously from observed communications and tied to **the window it was observed in and the observations that support it**. Where a statement is made, the basis for it is retained, so the follow-up question has an answer.

STRONG HERE**Controls with a network expression**

Inventory completeness, segmentation, communication security, remote and vendor access, unauthorised devices, and change appearing as new behaviour.

NOT THIS**Controls that live elsewhere**

Governance, training, physical security and supplier due diligence are not network events, and no amount of observation will evidence them.

Why it matters. Continuous evidence changes the assessment from a project into a review. It also changes the negotiating position: a continuous record traceable to observed traffic is considerably harder to challenge than a folder of screenshots dated the week before the auditor arrived.

WHERE THIS SHOWS UP

IEC 62443

Zone and conduit evidence taken from what actually crossed, not from the design.

ISO 27001, NIST CSF, NCA

Asset inventory and network control evidence accumulating between assessments.

HIPAA

Connected device inventory and segmentation evidence, without touching a device.

HOW TO TEST THIS

ASK ANY VENDOR

When your platform states a control is satisfied, what observation is behind it, and will that still be there in six months?

WHAT WE WOULD SHOW YOU

An evidence statement with its supporting observations and the window they were seen in, retained rather than regenerated.

NOTHING LEAVES

Run AI investigation inside an air-gapped network.

The usual trade is capability for connectivity. Isolated environments are told that modern tooling requires a cloud service, and so they go without.

THE SITUATION

Defence, national infrastructure, classified and many industrial environments have no outbound path by design. That is a deliberate control, not a gap to be worked around. Any capability that assumes a vendor cloud is simply unavailable, regardless of how good it is.

WHAT WIRETRACE DOES

Rumi, the WireTrace assistant, runs **entirely inside the customer environment**. The model is deployed within the network and reasons over the estate's own observed data. There is no external call and nothing to lose when the environment is isolated, so an air-gapped deployment behaves exactly like a connected one.

CONSEQUENCE**No residency conversation**

Nothing leaves, so there is no question about where it went, who processed it, or under whose jurisdiction it landed.

CONSEQUENCE**The investigation stays private**

During an incident the questions being asked are themselves sensitive. They stay inside the boundary along with the data.

Why it matters. This is an architectural property, not a configuration option. A platform designed around a cloud service cannot be made sovereign by switching something off, which is why this is worth testing directly rather than accepting as a claim.

WHERE THIS SHOWS UP

Defence and CNI

Networks with no outbound path by design, where a cloud service is simply unavailable.

Sovereign estates

Environments where data residency is a precondition rather than a preference.

Live incidents

Investigations where the questions being asked are themselves sensitive.

HOW TO TEST THIS

ASK ANY VENDOR

Which of your capabilities stop working if the environment has no outbound connectivity at all?

WHAT WE WOULD SHOW YOU

The assistant answering questions about your estate with the external path removed, because there was never one to remove.

ONE ESTATE, FOUR DOMAINS

Stop reconciling four tools that each see one quarter of the network.

Industrial, enterprise, connected and medical equipment usually end up under separate tools, separate teams and separate reports. The gaps between them are where the interesting traffic goes.

THE SITUATION

Domain-specific tooling produces domain-specific pictures. An engineering workstation that sits between the corporate network and the process appears in two of them, differently, and the relationship that matters most is the one that crosses the boundary between them. Reconciling the views is manual, perpetual and never quite finished.

WHAT WIRETRACE DOES

One sensor covers every domain present on the segment it watches, and one platform holds the whole estate. A relationship that crosses from enterprise into process is **a single observed relationship** rather than two half-views in two products that have to be matched up by hand.

OT

Controllers, relays, drives, historians and engineering workstations.

IT

Servers, endpoints, infrastructure and shadow systems.

IoT

Cameras, access control, building management and facility equipment.

IoMT

Clinical and diagnostic devices that cannot be touched.

Why it matters. Attacks do not respect the boundaries our tooling is organised around. The path from a corporate foothold to a process consequence crosses exactly the seam where two products stop talking to each other. One observed picture removes the seam.

Pick the use case that matches your problem

Each of these can be demonstrated against your own traffic in a scoped assessment. Tell us which one is the reason you are reading this, and we will build the evaluation around it rather than around a standard demonstration script.

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

WHERE THIS SHOWS UP

Mixed plants

A process network sharing infrastructure with corporate systems and facility equipment.

Hospitals

Clinical devices, building systems and enterprise IT on one physical estate.

Campus and city

Facilities where operational, connected and enterprise equipment have merged.

HOW TO TEST THIS

ASK ANY VENDOR

Is this one platform or several modules, and what is licensed separately per domain?

WHAT WE WOULD SHOW YOU

One sensor on a mixed segment covering industrial, enterprise, connected and clinical devices together, in a single picture.