FOR SECURITY, RISK AND OPERATIONS LEADERSHIP

The devices carrying your operational risk are the ones your tools cannot reach.

Most security programmes are measured on the estate they can see. The estate they cannot see is where the uncomfortable incidents begin: equipment that will not run an agent, cannot safely be scanned, and does not appear in any inventory anybody trusts.

THE GAP IN ONE PARAGRAPH

Agents cover devices that accept software. Scanners cover devices that tolerate being interrogated. In a modern estate, a large share of the equipment fits neither description, and it tends to be the equipment that runs the plant, treats the patient or controls the building.

The result is a visibility boundary that follows the tooling rather than the risk. Security reporting is confident about the managed estate and silent about the rest. When something happens outside that boundary, the first question in the room is what was even connected, and the honest answer is usually that nobody is certain.

WHAT CHANGES WITH WIRETRACE

WireTrace observes network traffic passively and reads what devices say to each other in their own protocols. From that it builds an inventory, identifies real exposure, and produces audit evidence, without installing anything on any device or sending a single packet onto the monitored network.

You know what you have
A live inventory derived from behaviour rather than from a spreadsheet, covering the managed estate and the unmanaged one on equal terms.

You know what is actually exposed
Weaknesses that were observed, prioritised by what is genuinely reachable and running, rather than a generic severity list to work through.

Audit stops being a project
Control evidence accumulates continuously from real communications, so an assessment becomes a report to review rather than a quarter of manual collection.

Incidents start from facts
When something happens, the first hour is spent on the question rather than on reconstructing what was connected and what it normally does.

WHO FEELS IT FIRST

The security leader
Accountable for an estate they can only partly see, and aware that the reporting reflects tooling coverage rather than actual risk. The unmanaged portion is the part that will be asked about after an incident.

The operations leader
Responsible for availability and safety, and rightly resistant to anything that touches running equipment. Needs visibility that carries no operational risk, or it will not be approved.

The compliance lead
Assembling evidence manually for each assessment, from interviews and screenshots that go stale immediately. Needs evidence that accumulates on its own and can be traced back to something real.

The uncomfortable version of the question. If you asked your team today for a list of every device connected to your operational network, how long would it take, how confident would they be in it, and how much of it would come from a document rather than from the network itself? The distance between that answer and reality is the exposure this addresses.

WHY IT IS ADOPTABLE

COMMON BLOCKER	WHY IT DOES NOT APPLY
"Operations will never approve it."	Nothing is installed on any device and nothing is transmitted onto the monitored network. The objection that stops scanning tools does not arise.
"We cannot send data to a vendor cloud."	The platform is fully on premises with no cloud dependency, and runs in fully air-gapped networks including its AI capability.
"We do not have a year for a rollout."	Connection is to a SPAN port or TAP. Assets begin appearing and classifying within minutes, with no agent programme to run.
"We already have tools."	WireTrace covers the part of the estate those tools structurally cannot reach, and feeds what it finds into them.
"Our environment is too mixed."	Industrial, enterprise, connected and medical devices are handled by one platform rather than by four tools that have to be reconciled.

WHERE THE VALUE LANDS

Risk reduction
The unmanaged estate stops being a blind spot, which is where most of the genuinely surprising findings are.

Operational cost
Inventory maintenance and audit evidence collection stop consuming skilled people who should be doing something else.

Regulatory position
Evidence is continuous and traceable to observed communications, which is a stronger position than a periodic manual assessment.

WHAT AN EVALUATION ACTUALLY INVOLVES

STAGE	WHAT HAPPENS	WHAT YOU NEED TO PROVIDE
Placement	We review your network diagram together and agree where visibility is worth the most, and what each position will and will not see.	A conversation with someone who knows the network.
Connection	A sensor is connected to a mirror port or TAP. Nothing is installed on any device and nothing is transmitted onto the monitored network.	A SPAN port or TAP, and rack space.
Observation	Assets appear and classify within minutes and the picture fills out as the environment goes through its normal cycles.	Time. Longer observation gives better behavioural context.
Findings	You receive what was found: the inventory, the exposure, and the evidence that could be produced, from your traffic.	A session to walk through it.

The test we would apply in your position. Ask any vendor to connect to one representative segment of your network and report what they found within a day, using your traffic rather than a demonstration environment. The gap between the inventory that comes back and the inventory you currently hold is the honest measure of the problem, whoever you end up buying from.

Start with one segment

A scoped assessment needs a mirror port and a short window. It returns what is actually on that segment, what is exposed, and what evidence can be produced from it. Most organisations find something in the first day that changes a plan.

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