SOLUTION BRIEF

Your agent coverage figure is measuring the wrong denominator.

Endpoint coverage is usually reported as a percentage of known devices. The number looks healthy because the denominator is the list of devices the tooling already knows about. Everything outside that list is not counted as uncovered, it is simply absent from the calculation.

The absent portion is not small, and it is not boring. Printers and multifunction devices, cameras and access control, building management, lab and test equipment, contractor laptops, appliances installed for a project and never decommissioned, and infrastructure that has been quietly running since before the current team arrived.

WHAT IS ACTUALLY IN THE GAP

Devices that cannot take an agent
Embedded and appliance-class equipment with no supported way to install anything, which nonetheless holds credentials, runs services and is reachable from the corporate network.

Devices nobody owns
Equipment procured by a department rather than by IT. It works, so nobody revisits it, and its firmware is whatever it shipped with.

Infrastructure that outlived its project
Test rigs, migration appliances and temporary systems still connected years after the work concluded, often with weak or default authentication.

Segmentation that has drifted
The design says these networks are separated. Individual exceptions, added for good reasons over several years, have made the separation partly theoretical.

WHAT WIRETRACE DOES HERE

WireTrace observes traffic passively and identifies every device that communicates, whether or not anything knows about it in advance. Because identification comes from behaviour rather than from an inventory lookup, the unmanaged estate is discovered on exactly the same terms as the managed one.

QUESTION	ANSWERED FROM OBSERVED TRAFFIC
What is on the network that we do not manage?	Every communicating device, with vendor, model and role derived from how it behaves.
Where is authentication weak?	Credentials passed in the clear and management interfaces reachable without protection, seen in traffic rather than inferred.
Is our certificate hygiene what we think?	Expired, self-signed and weak certificates actually in use, including on systems nobody remembers deploying.
Do our network boundaries hold?	What genuinely crosses between segments, compared with what the design intends.
What talks outside, and why?	External communication relationships, including devices reaching manufacturer services nobody approved.

This is a complement, not a replacement. Your endpoint and detection tooling covers the managed estate well. WireTrace covers the part it structurally cannot reach, and feeds what it finds back into the same workflow. The intended outcome is that the coverage figure becomes honest, not that a tool gets replaced.

WHERE IT IS USED

USE CASE

Reconciling the CMDB against reality

An observed inventory compared with the recorded one is usually a short and uncomfortable meeting, and it is the fastest way to establish how much of the estate is genuinely under management.

USE CASE

Making a segmentation project finishable

These projects stall on the question of what will break. Observed relationships answer it with data, and then show whether the implemented boundary is actually holding.

USE CASE

Governing the building estate

Cameras, access control and building management sit on the corporate network with the security posture of appliances. They become visible, attributable and monitorable.

USE CASE

Preparing for certification

Asset management and access control evidence assembled continuously from communications, rather than reconstructed manually before each assessment.

USE CASE

Supporting merger and acquisition work

When an unfamiliar network arrives, connecting passively and observing is the fastest safe way to learn what was acquired, without credentials or cooperation.

USE CASE

Giving investigations a starting point

When an alert names an address, the device identity, its normal behaviour and its usual peers are already recorded, which removes the slowest part of triage.

FITS THE WAY YOU ALREADY WORK

No endpoint change

Nothing installed, no build image to modify, no rollout programme to schedule.

No scan windows

Nothing transmitted onto the network, so there is no change approval to negotiate.

Feeds existing tooling

Inventory, findings and context delivered to the platforms your teams already use.

WHAT TENDS TO TURN UP IN THE FIRST WEEK

These are the findings that recur across enterprise assessments. None of them is exotic, and that is the point: they persist because nothing was looking in the places they live.

- ✓ Devices communicating that appear in **no inventory anyone maintains**
- ✓ Credentials still passed **in the clear** by embedded equipment
- ✓ Equipment reaching **manufacturer services** nobody approved
- ✓ Management interfaces reachable from **general user networks**
- ✓ Certificates **expired years ago** and still in active use
- ✓ Traffic crossing a boundary that is **documented as closed**

REGULATORY CONTEXT

Evidence is mapped to the frameworks enterprises are assessed against, including **ISO 27001**, **NIST CSF 2.0** and the national frameworks applicable in each market, such as the **NCA ECC** controls in the Kingdom of Saudi Arabia. Asset management, access control and network security controls benefit most, because they are the ones where observed traffic is genuinely better evidence than a document.

Point it at one campus segment

A mirror port and a short observation window will tell you how large the gap between your inventory and your network actually is. That number tends to decide the conversation on its own.

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