

SOLUTION BRIEF

Most security platforms answer to a cloud you do not control.

For a national operator the first question is not what a platform detects. It is where the data goes, who can reach it, what happens when the link is cut, and whether the vendor retains any capability over the deployment after handover. Those questions eliminate most of the market before a technical evaluation begins.

WireTrace was built to be deployed inside the boundary and to stay there. Fully on premises, no cloud dependency, no outbound requirement, and no reduction in capability when the environment is isolated.

WHAT SOVEREIGNTY HAS TO MEAN IN PRACTICE

The data does not leave

No telemetry to a vendor service, no external analysis, no update path that requires reaching out. What is observed inside the boundary stays inside the boundary.

Isolation is a supported model

Air-gapped operation is a first-class deployment rather than a degraded mode. Analytics and the AI assistant run inside the network with no external dependency.

The operator retains control

The platform is operated by the customer. There is no vendor-held capability over a deployed system and no external administrative path into it.

Evidence stays local and auditable

Observations, findings and compliance evidence are held within the environment, which is what a national regulator expects to be shown.

WHY PASSIVE MATTERS AT NATIONAL SCALE

Critical infrastructure networks combine the constraints of every other environment at once. Generation, transmission, water, transport and telecommunications estates all carry equipment that cannot be scanned, cannot host software and cannot tolerate interruption, frequently under a legal duty of continuity. Passive observation is not merely the safer option here, it is often the only technique that is permitted at all.

REQUIREMENT	HOW WIRETRACE MEETS IT
Know the national estate	A live inventory of every communicating device across sites, derived from observation rather than from operator-maintained records.
No interference with operations	Nothing transmitted onto monitored networks and nothing installed on any device, so continuity duties are unaffected.
Work without connectivity	Full capability inside isolated networks, including at sites with no external link by design.
Demonstrate compliance to a regulator	Continuous control evidence drawn from observed communications and mapped to the applicable national framework.
Cover many sites, one picture	Distributed sensors reporting to a central platform, with separation between organisations or authorities where required.
Understand supply chain access	Vendor, integrator and support connections into the estate become visible, including the ones agreed commercially and never documented.

WHERE IT IS USED

USE CASE

Establishing a national asset picture

Sector regulators increasingly ask operators what is connected to critical systems. Observation produces an answer that is current and traceable rather than assembled from returns.

USE CASE

Supervising a multi-operator sector

Separated environments within one platform allow an authority or a shared service to cover several operators without merging their data.

USE CASE

Watching the supply chain path

Foreign and third-party support access into national systems is a standing concern. Observed traffic shows who connects, to what, and what happens during the session.

USE CASE

Assurance in classified environments

Networks that cannot connect outward still need modern visibility. Running fully inside the boundary makes that possible without an exception process.

USE CASE

Regulator-ready reporting

Evidence produced continuously from communications, with the observations retained, which is a materially stronger position than a periodic self-assessment.

USE CASE

Incident support without external help

Protocol history and device behaviour are already held locally, so investigation does not depend on sending anything to an external party.

REGULATORY CONTEXT

Evidence is mapped to the frameworks national operators are assessed against. In the Kingdom of Saudi Arabia that includes the **NCA ECC** and, for operational environments, the **NCA OTCC** controls; internationally it includes **NIST CSF 2.0**, **IEC 62443-3-3** for industrial systems, **NERC CIP** for bulk electric system operators and **ISO 27001**. Each mapping is explicit about what network observation can and cannot evidence, which is the honest basis for a regulatory conversation.

Procurement questions we expect, and welcome. Where is data stored and for how long. What reaches the vendor, and the answer is nothing. What happens in a full network isolation, and the answer is that the platform continues to work. Who can administer a deployed system. What the update path is in an air-gapped environment. These are the right questions and they are the reason this platform is shaped the way it is.

DEPLOYMENT SHAPE

Single authority or site

Sensors and platform inside one boundary, operated entirely by the customer.

National, multi-site

Distributed sensors reporting to a central platform, with one estate-wide position.

Fully air-gapped

Complete capability with no outbound path, including analytics and the AI assistant.

Begin with one operator, one site

A scoped assessment demonstrates the model where it matters: inside the boundary, transmitting nothing, producing an asset picture and evidence that never leaves the environment. It is also the fastest way to test our sovereignty claims rather than take them on trust.

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