THE CATEGORY

Deep packet inspection tells you a protocol was there. That stopped being useful a decade ago.

Recognising Modbus on the wire is a solved problem. Every serious network tool can label the traffic, count the sessions and draw the graph. The label is not the intelligence, and treating it as the finish line is why so many organisations own a tool that identifies protocols and still cannot answer basic questions about their own estate.

Deep Protocol & Asset Intelligence begins where identification ends. It reads what the conversation contained, works out what the participants are, learns what normal looks like for each of them, and keeps the evidence.

THE DISTANCE BETWEEN THE TWO

QUESTION	DEEP PACKET INSPECTION	DEEP PROTOCOL & ASSET INTELLIGENCE
What is this traffic?	Modbus, on port 502.	Modbus, and here is the function being called, the register range being written, and which side initiated it.
What are these devices?	Two IP addresses.	An engineering workstation writing to a named controller model on known firmware, positioned in the process it serves.
Is this normal?	Traffic volume is within range.	This initiator has never written to this device before, and this command type is new for this relationship.
Can you prove it?	Here is a flow record.	Here is the control this supports, the observation window, and the communications the statement rests on.

The distinction matters commercially, not just technically. A protocol label produces a dashboard. Asset identity, behavioural context and retained evidence produce an inventory the operations team trusts, a risk position the security team can act on, and an audit position the compliance team can defend. Those are three budgets, and they are why the difference is worth understanding before selecting a tool.

FOUR PILLARS

PILLAR 1

Protocol depth

More than 250 protocols read for their content and meaning, not merely classified. Industrial control, building systems, medical, enterprise and network management, including the field protocols that general-purpose tools treat as opaque traffic.

PILLAR 2

Asset identity

Identity assembled from everything a device reveals across every protocol it speaks, rather than inferred from a single signal. The result is a device record with a vendor, a model, a role and a firmware version attached to it.

PILLAR 3

Behavioural context

What normal looks like for this device, on this protocol, with these peers. Meaningful change is judged against a device's own history, which is what separates a real signal from an alert about a busy afternoon.

PILLAR 4

Evidence

Observations retained with the context that makes them defensible later, so a finding can be explained to an engineer, an auditor or an investigator months after the traffic itself has gone.

WHY PASSIVE IS THE HARDER ENGINEERING PROBLEM

Active tools have it easy. They ask a device what it is and read the answer. That works until the device is a protection relay, a ventilator or a controller that predates the idea of being asked anything, at which point the question is unsafe and the technique is unavailable.

Observing has no such fallback. Everything must be derived from what devices volunteer to each other in the course of doing their jobs. **Doing that well requires understanding the protocols at the level of their meaning**, which is precisely the work most tools skip, and precisely why they end up needing an agent or a scan to fill the gap.

FROM OBSERVATION TO OUTCOME

Network
Your existing infrastructure

→

SPAN or TAP
Passive mirror, nothing transmitted

→

Deep protocol analysis
What was said, not just who spoke

→

Asset & communication intelligence
Identity, relationships, behaviour

→

Security, operations, compliance
Decisions and evidence

WHAT THE PLATFORM PRODUCES

Asset intelligence

A live inventory with vendor, model, role and firmware, covering managed and unmanaged devices alike, updated as the estate changes rather than as someone remembers to update a spreadsheet.

Communication intelligence

The real relationship map: who talks to whom, over what, in which direction, and what that traffic contains. The basis for segmentation work that reflects the network as it is.

Exposure intelligence

Weaknesses observed rather than assumed: credentials in the clear, certificates that should have been replaced, management interfaces reachable from places they should not be. Vulnerability correlation is driven by observed firmware and reachability, so prioritisation reflects the estate you have.

Compliance intelligence

Control evidence assembled continuously from observed communications and mapped to the frameworks you are assessed against, with the observations behind each statement retained.

PROTOCOL COVERAGE ACROSS THE ESTATE

Industrial

Process control, energy, manufacturing and safety protocols, read for commands and values rather than counted as sessions.

Medical

Clinical imaging and messaging exchanges including DICOM and HL7, handled with the sensitivity a patient environment demands.

Enterprise

Directory, transport, web, file, mail and remote access protocols, including the security-relevant detail inside them.

Infrastructure

Discovery, management, routing and building system protocols that describe how the network is actually put together.

Rumi, private AI inside your network. Investigation assistance that runs entirely within the customer environment, including air-gapped ones. It answers questions about your estate using your own observed data, with no cloud service behind it and nothing leaving the boundary. Organisations that cannot send telemetry to a vendor cloud do not have to give up modern tooling to stay compliant.

HOW TO EVALUATE A CLAIM IN THIS SPACE

Whatever you end up buying, these questions separate protocol identification from protocol intelligence. They are worth asking of every vendor on the list, including us.

DEPTH
For a protocol I care about, what do you extract beyond the fact that it appeared? Show me a real conversation and what you understood from it.

IDENTITY
How do you establish a device's model and firmware without an agent and without scanning it? Show me on a device you have never seen before.

METHOD
Which capabilities need active scanning, endpoint agents, additional modules or a cloud connection? Which work in a fully isolated network?

EVIDENCE
When your platform states something for an auditor, what observation is behind it, and is that still available in six months?

Bring us a protocol you think nobody reads properly

The most useful technical conversation we can have is not a slide deck. Choose a segment of your network, or a protocol your current tooling treats as opaque, and let us show you what is recoverable from it passively. That is a short exercise and it settles the question quickly.

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