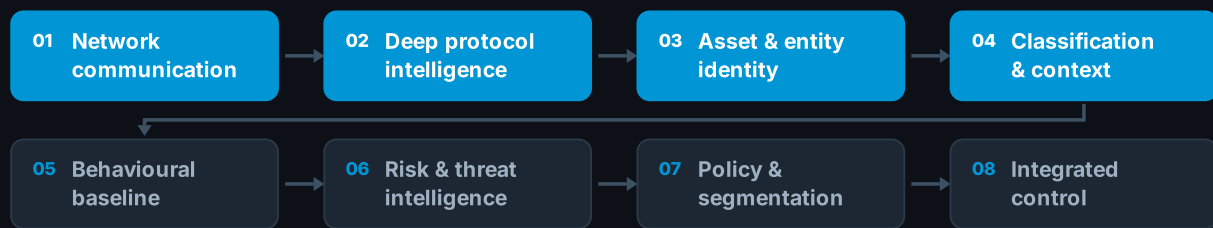


SOLUTION BRIEF

Asset Intelligence

How WireTrace knows what every device on your network is: identity read from what devices state about themselves, held as one durable record per device, classified with stated confidence, and honest about what it cannot see.



For: Security architects, OT engineers, asset owners, IT operations

An asset inventory is only as good as the evidence behind each line. Spreadsheets go stale, agents cover only the machines that can run them, and an IP address says where a device was, not what it is. WireTrace answers the question from the network itself: **it reads what each device states about itself, joins that evidence into one durable identity, and shows where every value came from.**

250+

protocols decoded to the payload, the source of device-stated identity

1

durable identity per physical device, across address changes, interfaces and sensors

600+

built-in classification rules, extended by your own no-code rules

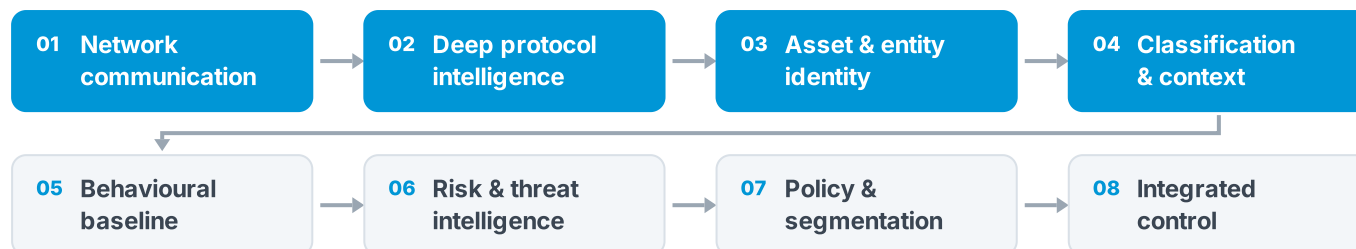
150+

cloud, SaaS, vendor-cloud and infrastructure applications recognised

01 Why device identity is hard

Most networks carry IT, OT, IoT and medical devices (IoMT) side by side, and each resists a different part of the usual toolset. Controllers and medical devices cannot carry an agent and should not be scanned. Laptops change address every day. Virtual machines are cloned from one image with identical identifiers. A record keyed on an address, a host name or a guess will merge two devices that should be separate, or split one device into several.

WireTrace takes a different approach. It is a **Deep Protocol & Asset Intelligence (DPAI)** platform: it decodes network communication down to the protocol fields that carry a device's own description of itself, and builds identity only from evidence it can state and defend.



The WireTrace platform flow. Highlighted layers are the subject of this document.

02 Passive discovery

WireTrace builds and maintains the asset inventory from mirrored traffic, taken from a SPAN port, network TAP or ERSPAN session. The capture interface only receives; it never transmits onto the monitored network, and nothing is installed on the devices being observed. Sensors at each site report to one central platform, which keeps one de-duplicated inventory.

Each device gets a profile: addresses, protocols, peers, first and last seen, classification, and the source of each value. Discovery is as complete as the traffic the sensors see, so sensor placement is part of every deployment plan.

03 Deep protocol identity

WireTrace decodes protocol payloads, not just headers. Many industrial, building and network protocols carry the device's own identity record, and WireTrace decodes these and uses them as primary evidence. Examples include the identity object an EtherNet/IP device returns, PROFINET station names and identification data, the BACnet device object, the component identity a Siemens S7 controller reports, and the system description a network device publishes over SNMP. WireTrace records which observed evidence produced each attribute.

WireTrace observes: a programmable controller

- An engineering workstation reads the controller's identity over S7comm
- The reply carries the vendor, order number, firmware version and serial number
- The controller answers reads and writes from a supervisory server and one workstation

WireTrace produces

- Manufacturer, normalised to one name, with the order number and firmware the controller stated
- A durable identity anchored on the stated serial number, graded Strong
- Type PLC, domain OT, Purdue level 1, with a confidence and a one-line reason
- Its peers, protocols and connection history, and the firmware available for advisory matching

04 Durable device identity

Addresses change; devices do not. WireTrace keeps **one durable identity per physical device**, even when its IP address changes, or it is seen on several interfaces or by several sensors.

WireTrace observes: a workstation whose address changes daily

- A new DHCP lease each morning, with the same client identifier and host name
- The same name resolved over DNS and announced over NetBIOS
- A domain sign-in, and connections to collaboration and cloud services
- A legacy application sending a password in clear text

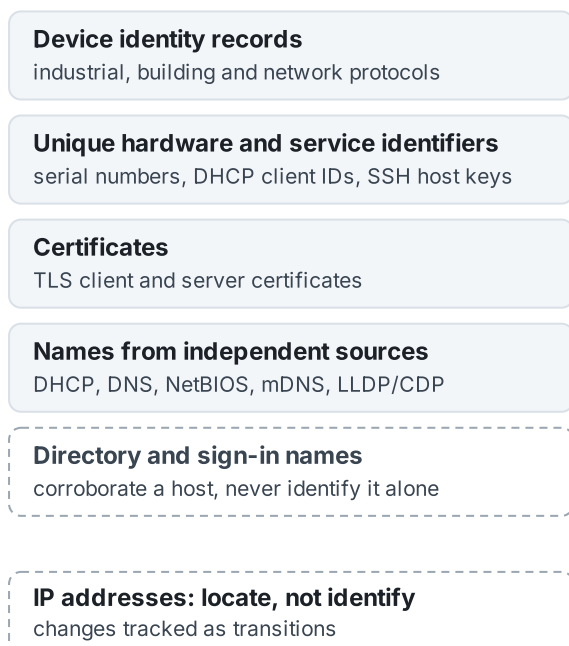
WireTrace produces

- One device, not a new record per lease, with each address held as a time-bounded binding
- Operating system inferred with a stated confidence
- The cloud and SaaS applications it uses, recognised from the names it resolves and connects to
- An observed-credential exposure finding, so the weak practice can be fixed

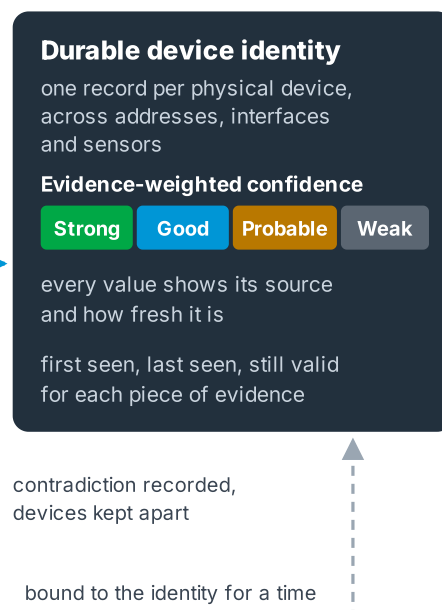
Joins only on unique, corroborated, device-stated evidence

Identity combines many independent kinds of evidence: device-stated hardware and protocol identifiers, DHCP client identifiers, SNMP engine identifiers, SSH host keys, certificates, and names from DHCP, DNS, NetBIOS, mDNS, LLDP/CDP and directory protocols. Each kind of evidence carries a stated strength. Records are joined only on values a device states uniquely. A host name needs corroboration from an independent source. Directory and sign-in names corroborate a host; they never identify it alone. An IP address locates a device but never identifies it.

EVIDENCE THE DEVICE STATES



ONE DURABLE IDENTITY



The identity evidence model. Unique evidence the device states is joined into one durable identity with a confidence. Values that are not unique are refused, and addresses are attached to the identity for as long as the evidence supports them.

Clone safeguards and time-aware identity

When two devices present the same supposedly unique value, whether from a cloned image, a vendor default or a gateway relaying a downstream device, WireTrace refuses to merge them blindly and records the contradiction. Identity evidence is time-bounded: first seen, last seen and still valid. Address changes are tracked as transitions, not conflicts, and stale bindings expire safely. Before any automated action, WireTrace checks that the target is identified well enough, and recently enough, to act on safely.

Evidence-weighted confidence

Every identity carries an evidence-weighted confidence, graded Strong, Good, Probable or Weak. The grade is available through the API; the console shows each identity value with its source and freshness. Strong identities rest on a stable hardware or protocol identifier; devices that state none grade lower, and WireTrace says so.

05 Classification and context

WireTrace classifies devices by **domain** (IT, OT, IoT, medical and network), **device type** (for example PLC, RTU, protection relay, HMI, engineering workstation, switch, camera, printer) and **role**, each with a confidence, using 600+ built-in classification rules and a hierarchical device taxonomy. Devices are placed on a **Purdue level** with a stated confidence and a one-line reason. Classifications show their confidence and the evidence behind them. A device the evidence cannot place stays unknown; it is not guessed.

Administrators write their own classification rules in a no-code editor, for site-specific equipment or naming conventions. A preview shows what would change before anything is applied.

WireTrace observes: an IP camera

- ONVIF device information announcing manufacturer, model and firmware
- A DHCP request and an mDNS announcement with the same device name
- Regular connections to the manufacturer's cloud service

WireTrace produces

- Type IP camera, domain IoT, with confidence and the evidence behind it
- Manufacturer, model and firmware, each with its source
- The vendor-cloud application it uses, recognised from the catalogue
- A visibility statement: which evidence is present and what is missing

Attribute	How WireTrace establishes it
Manufacturer	Identified from what the device states on the network, normalised to one name. When a device states nothing, a low-confidence fallback to the network-card maker is used and labelled as such.
Model, firmware, serial	Where a device states its model, firmware or serial number, as many industrial controllers, IoT and network devices do, WireTrace records it with its source. Credentialed collection and switch polling add these details for IT and network equipment. Not every device reveals them passively.
Operating system	Inferred passively with a stated confidence. An OS the device announces itself takes precedence, and credentialed collection adds the exact version.
Applications	150+ cloud, SaaS, vendor-cloud and infrastructure applications recognised with confidence. You can add your own.
Observed credentials	Account names and credentials exposed by clear-text and legacy authentication, such as HTTP basic authentication or LDAP simple binds, are detected so weak practices can be fixed. Revealing a captured secret is restricted to authorised roles.

Attribute	How WireTrace establishes it
Peers and communications	Who the device talks to, over which protocols and ports, its top peers and its connection history. Optional modules add a zone-to-zone communication matrix and a Purdue-level view.
Visibility assurance	For each device, which kinds of evidence are present, missing or stale. An empty result is never presented as a clean one.

06 Optional, governed enrichment

- **Switch and router polling.** With read-only SNMP access, WireTrace adds port-level connectivity, neighbour relationships and hardware details from switches and routers. Switches also feed the Network Digital Twin, a live physical map of the network.
- **Credentialed collection for IT hosts.** For hosts an administrator chooses to scan with credentials, WireTrace collects installed software, services, accounts and hardware. Passive traffic gives software hints, not an installed-software list.
- **Governance.** Enrichment needs defined scopes and read-only credentials, runs from the management interface rather than the capture interface, and an OT-safe profile keeps probes away from industrial and medical devices unless explicitly allowed.

07 How the intelligence improves

Asset identity and classification knowledge is maintained as versioned content, separate from product code, and improved with each release. The Platform Updates page shows the version and freshness of each intelligence area.

Limits, stated plainly

- WireTrace sees what reaches its sensors. Devices behind routers appear by address unless enrichment adds more.
- Model, firmware and serial number are recorded where devices state them, or where optional enrichment collects them. Installed software comes only from hosts you scan with credentials.
- Identity confidence follows the evidence. Devices that state no unique identifier grade Probable or Weak, and some devices stay unclassified rather than being guessed.
- Addresses or interfaces are joined into one device only where the evidence proves it. Address translation, redundant pairs and clusters are not modelled.
- WireTrace does not decrypt traffic. Encrypted sessions still yield certificate, fingerprint and behavioural evidence.

See your own inventory take shape

Connect a WireTrace sensor to one SPAN or TAP. The first devices appear within minutes, each with the evidence behind its identity, and the inventory deepens as more of the network is observed.

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