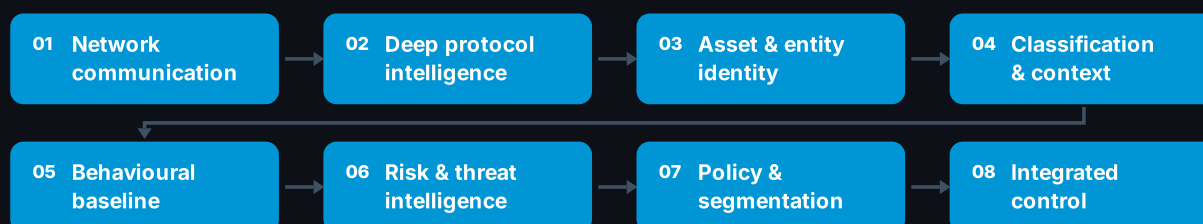


WIRETRACE PLATFORM OVERVIEW

Know every device. See what matters. Act with control.

Your network is talking. Start listening. WireTrace turns what every device says on the network into durable identity, risk, policy and action, across IT, OT, IoT and medical devices, on your own infrastructure.



For: CIO, CISO, security and OT leadership, partners

Most organisations can name the laptops and servers they manage. Far fewer can name the controllers, building systems, cameras, medical devices, printers and appliances that share the same network, or say what those devices are doing. Yet every one of them describes itself every time it communicates. **WireTrace listens deeply enough to understand it.**

250+

protocols decoded to the payload, across IT, OT, IoT and medical devices

1

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

90+

detection rules mapped to MITRE ATT&CK and ATT&CK for ICS

Minutes

from a mirrored port to the first identified devices

01 The problem: the devices carrying your risk are the ones your tools cannot see

Endpoint agents cover the machines that can run them. Vulnerability scanners cover the machines that can safely be scanned. Configuration databases cover the machines someone remembered to record. What is left over (programmable controllers, protection relays, building management systems, infusion pumps, imaging modalities, cameras, badge readers, uninterruptible power supplies, embedded appliances) is often the most operationally critical part of the estate, and the least understood.

Unknown devices

Inventories built from agents and spreadsheets miss what cannot carry an agent, and drift the moment the network changes.

Shallow context

An IP address and an open port do not say that a device is a safety controller running end-of-life firmware that an engineering workstation reprogrammed last night.

Decisions without evidence

Segmentation, vulnerability and audit decisions are taken on assumptions about how devices communicate, rather than on what the network shows.

02 What WireTrace is

WireTrace is a **Deep Protocol & Asset Intelligence (DPAI)** platform. It reads the network communication your devices already produce, decodes it to the level of individual protocol fields, and builds from that evidence a living, explainable understanding of every device: what it is, what it does, who it depends on, what puts it at risk, and whether its behaviour matches your intent.

Conventional deep packet inspection answers the question *"which protocol was this?"* DPAI answers the questions security and operations teams actually ask: *which device is this, who made it, what firmware is it running, what is it being told to do, is that normal, and what should we do about it?*

The platform flow on the cover shows how it works. Each layer builds on the one before it, which is why WireTrace is a platform rather than a set of separate tools. The same durable device identity that powers the inventory also scopes a detection, prioritises a vulnerability, anchors a segmentation rule and travels with an alert into your SIEM.

03 Four outcomes

Know every device

A continuously maintained inventory across IT, OT, IoT and medical devices, built from what devices state on the network. Each device keeps one durable identity even as its address changes, is classified by type, role and Purdue level, and shows manufacturer, model and firmware wherever the device reveals them. Every value carries its source and a confidence.

See what matters

Vulnerabilities matched to each device's identified software and firmware and prioritised by known exploitation, exposures such as clear-text credentials and weak cryptography, end-of-life technology, and a 0-100 Asset Risk Score that explains its own reasoning.

Detect and investigate

More than 90 deterministic detection rules covering IT threats, industrial command misuse, ransomware staging and network-integrity attacks, mapped to MITRE ATT&CK and ATT&CK for ICS. Analysts triage in one queue and open investigations that assemble the evidence, timeline and supporting and contradicting facts.

Act with control

Baselines of how devices and protocols normally communicate, segmentation intent expressed as traffic rules and IEC 62443 zones, continuous violation detection, and governed automation with approvals, safety limits and an append-only activity log. Decisions reach the tools you already run through syslog, webhooks, email and a REST API.

04 What makes the intelligence different

Depth: payloads, not headers

WireTrace decodes more than 250 protocols to the level of their fields: the order number and firmware a controller reports, the station name in an industrial frame, the function code an engineering workstation sends, the certificate a medical gateway presents. Many industrial, building and network protocols carry the device's own identity record, and WireTrace uses it as primary evidence.

Identity: one device, many addresses

Addresses change; devices do not. WireTrace joins evidence only on identifiers a device states uniquely (a controller serial number, a switch bridge identifier, an SSH host key, a DHCP client identifier, a certificate) and refuses values that are cloned, defaulted or relayed by another device. The result is a durable identity that survives DHCP churn, roaming and multiple sensors, with an evidence-weighted confidence.

Explainability: every conclusion shows its evidence

Classifications, identities, detections and risk scores state where they came from and how confident they are. WireTrace also states what it cannot see for each device, so an empty result is never mistaken for a clean one.

Breadth: one platform across four domains

IT, OT, IoT and medical devices are understood by one engine, in one inventory, under one policy model. The converged reality of modern networks, where an engineering laptop, a cloud-connected camera and a protection relay share a path, is visible as it actually is.

05 Built for the networks that matter most

Environment	What WireTrace brings
Manufacturing, energy, utilities, oil and gas	Controller and field-device identity from industrial protocols, Purdue-level mapping, monitoring of writes, program transfers and mode changes, segmentation evidence for IEC 62443 and NERC CIP.
Healthcare	Identification of connected medical devices alongside clinical IT and building systems, with patient values masked inside the sensor.

Environment	What WireTrace brings
Government and critical national infrastructure	Full operation without internet access, on customer infrastructure, with offline refresh of threat and vulnerability data.
Facilities, airports and data centres	Building automation, power and access-control systems treated as the control systems they are.
Enterprise IT and campus	Unmanaged and shadow devices, cloud and SaaS usage per device, clear-text credential exposure, and asset context for the SOC.

06 Deployment and trust

Passive by default

Sensors attach to 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.

Optional, governed enrichment

Where you choose, administrators can add read-only switch polling and credentialed collection for IT systems. Enrichment runs from the management interface, within scopes you define, and an OT-safe profile keeps probes away from industrial and medical devices unless explicitly allowed.

On your infrastructure

WireTrace installs on servers or virtual machines you own. Storage, analysis and the private AI assistant all run there. External intelligence feeds are optional.

Air-gap capable

The platform runs fully without internet access. Threat and vulnerability data can be refreshed through an offline collection bundle that you carry across under your own transfer controls.

07 Fits the way you already work

WireTrace is the intelligence and decision layer; it is designed to strengthen the controls you already operate rather than replace them.

- **Security operations:** alerts to any SIEM over syslog (CEF, LEEF, RFC 5424) or the Splunk HTTP Event Collector, JSON webhooks for automation, email and SNMP traps.
- **Enforcement:** segmentation intent, violations and proposed block rules handed to your firewall, NAC and network teams through rule exports, notifications and the API. Your existing controls enforce.
- **Data access:** a read-only REST API with OAuth 2.0 client credentials, scoped tokens and IP allowlists, running on your appliance.
- **Identity:** sign-in through LDAP and Active Directory or OpenID Connect single sign-on.
- **Compliance:** network evidence mapped to 415 controls across seven frameworks, with auditors closing the remainder inside the platform.

08 Rumi, the private AI assistant

Rumi runs entirely on the WireTrace server, with no external AI service. It answers questions about your environment in plain language, explains why a device was classified or scored as it was, and summarises investigations. Facts, counts and rankings come from deterministic queries with click-through evidence;

the language model only words the answer. Rumi assists analysts; it does not take decisions on their behalf.

Limits, stated plainly

- WireTrace sees what reaches its sensors. Coverage follows sensor placement.
- It does not decrypt traffic. Encrypted sessions still yield identity, certificate and behavioural evidence, but not their content.
- Model and firmware are recorded where devices state them, or where optional enrichment collects them; not every device reveals them passively.
- WireTrace defines, validates and monitors segmentation intent. Your firewalls, NAC and switches enforce it.

Start with one mirrored port

A WireTrace evaluation starts passively on a single SPAN or TAP. Within minutes the first devices appear; within days you have an inventory, a communication map and a prioritised list of what deserves attention.

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