Frequently Asked Questions

Answers to the most common questions from prospects and customers about WireTrace deployment, capabilities, pricing, compliance, and technical architecture.

PLATFORM & CAPABILITIES

What is WireTrace?
WireTrace is a passive network intelligence platform that discovers, classifies, and monitors every device on your network by analyzing raw traffic. It provides asset inventory, protocol intelligence, security insights, threat detection, vulnerability prioritization, and compliance evidence - across IT, OT, IoMT, and IoT environments - without agents, active scanning, or cloud dependency.

How does WireTrace discover assets?
By passively observing network traffic from a SPAN port or TAP. The DPI engine parses 250+ protocols and extracts device identity from protocol fingerprints, MAC addresses, DHCP hostnames, TLS certificates, mDNS/SSDP announcements, and behavioral patterns. Multi-signal weighted voting produces confident classifications - **not just MAC OUI guesses**.

What does "wire-level protocol dissection" mean?
WireTrace reads the actual payload of network protocols - Modbus function codes and register values, S7Comm PLC parameters, TLS certificate fields, DNP3 control commands, HL7 clinical messages. This is fundamentally different from port-based identification. **The difference between seeing "traffic on port 502" and knowing "a Write command was sent to register 40001."**

Does WireTrace send any traffic on the monitored network?
Not from the capture interface - it is receive-only. The sensor observes a copy of traffic from a SPAN port or TAP, and zero packets are transmitted onto the monitored network from it. Optional SNMP enrichment and Bahith active scanning, when an operator enables them, transmit from the management interface only and are off by default. This makes WireTrace safe for OT, medical, and safety-critical environments.

How many protocols does WireTrace support?
250+ and continuously expanding. This includes industrial (Modbus, S7Comm, DNP3, EtherNet/IP, PROFINET, BACnet, OPC-UA, and more), medical (DICOM, HL7, Philips, Draeger, GE CARESCAPE, Hamilton, Masimo, Abbott, and more), enterprise (TLS, SSH, RDP, SMB, DNS, LDAP, Kerberos, SNMP, and more), and IoT (SSDP, mDNS, LLDP, CDP, and more). Each parser performs deep field extraction, not just port identification.

Can WireTrace identify medical devices by vendor and model?
Yes. WireTrace parses proprietary medical device protocols from major manufacturers. Ventilators, patient monitors, infusion pumps, anesthesia machines, imaging systems, and lab analyzers are identified by manufacturer, model family, and clinical function from observed protocol communications.

DEPLOYMENT

How long does deployment take?
Server installation: **under 10 minutes** using the self-extracting installer. Sensor deployment: **under 60 seconds** per sensor. First assets classified: **within 30 seconds** of traffic observation. No professional services engagement required.

What do I need to deploy?
One server (physical or VM running Ubuntu 22.04/24.04), one or more sensors connected to SPAN ports or network TAPs, and network connectivity between sensors and server. No agents on endpoints. No internet required. See the Deployment & Sizing Guide for hardware specifications.

Does WireTrace work in air-gapped environments?
Yes. Fully air-gap deployable. All features operate without internet connectivity - discovery, classification, compliance evidence, threat detection, and reporting. The self-extracting installer contains everything needed. No cloud dependency for any functionality.

Can I monitor multiple network segments?

Yes. Deploy one sensor per segment - each connects to a SPAN port or TAP on the segment you want to monitor. All sensors report to a centralized server. Supports campus, multi-building, multi-site, and mixed OT/IT/IoT topologies.

SECURITY & COMPLIANCE

Which compliance frameworks does WireTrace support?
7 frameworks - IEC 62443, ISO 27001, HIPAA, NCA ECC, NCA OTCC, NIST CSF 2.0, and NERC CIP - plus custom frameworks. Evidence is generated continuously from observed traffic - asset inventories, communication flows, segmentation validation, encryption posture, and access control documentation. Replaces manual evidence collection.

How does WireTrace generate compliance evidence?
By observing actual network behavior. Asset inventories come from observed protocol communications. Segmentation evidence comes from documented cross-zone traffic. Encryption posture comes from observed TLS negotiations. **Everything is derived from what the network actually does - not from self-reported questionnaires.**

How does vulnerability prioritization work?
WireTrace matches discovered assets against CVE databases (NVD, CISA KEV) with EPSS risk scoring. Vulnerabilities are **ranked by observed exposure** - which protocols are active, which firmware versions are running, which services are exposed. Not by theoretical scan results.

Is my data secure?
All data stays on-premises. No telemetry, no cloud sync, no external data transmission. Sensor-to-server communication is cryptographically signed. The platform uses JWT authentication with RSA key pairs, role-based access control, multi-tenant data isolation, and LDAP/AD/OIDC SSO integration.

PRICING & LICENSING

How is WireTrace licensed?
Per-asset, subscription-based. Pricing scales transparently with the number of monitored devices. Every subscription includes the full platform - all protocol intelligence, all compliance frameworks, all capabilities - with continuous updates throughout the subscription period.

Are there module add-ons or feature tiers?
No. Every subscription includes all capabilities: asset discovery, protocol intelligence, security insights, threat detection, vulnerability prioritization, behavioral baselines, compliance evidence, and reporting. No feature fragmentation, no module upgrades, no hidden costs.

Can I try WireTrace before purchasing?
Yes. We offer proof-of-value deployments. Connect a sensor to a SPAN port on your network and see your own assets, protocols, and security findings within 30 seconds. No commitment required. Contact **sales@wiretrace.io** to schedule.

INTEGRATION

What integrations does WireTrace support?
REST API for all data endpoints, **syslog forwarding** and **CEF** for SIEM integration, **STIX/TAXII** for threat intelligence exchange, **webhooks** and **email alerts** for notifications, **CSV export** for data extraction, **firewall rule generation** (PAN-OS, FortiGate), and **LDAP/AD/OIDC SSO** for authentication.

Does WireTrace support multi-tenancy?
Yes. Multi-tenant architecture with role-based access control. Managed service providers can monitor multiple customers from a single console with isolated data per tenant.

What operating systems are supported?
Server and sensor run on **Ubuntu 22.04 LTS and 24.04 LTS**. Supported on physical hardware, VMware ESXi, KVM/QEMU, Hyper-V, and Proxmox. All components run as containers; the installer provisions the container runtime automatically if it is not already present.

Have More Questions?

Contact the WireTrace team. sales@wiretrace.io