WIRETRACE

PLATFORM DATASHEET

Passive Digital Asset Intelligence

WireTrace gives security teams complete visibility into every device on their network - IT, OT, IoMT, and IoT - without agents, active scanning, or cloud dependency. By analyzing raw network traffic passively, WireTrace builds a continuously updated asset inventory, identifies security exposures, generates compliance evidence, and detects threats. One platform. Every environment. Zero disruption.

250+	30s	100%	0
Protocol Parsers	First Asset Classified	Passive	Agents Required

Why WireTrace is Different

- **Passive-Only Architecture** - Zero network disruption. No active probes, no scanning, no interrogation. Safe for OT, medical, and safety-critical environments.
- **Unified IT / OT / IoMT / IoT Visibility** - One platform across all environments. No separate tools for industrial, medical, enterprise, and IoT domains.
- **Deep Protocol Intelligence** - 250+ DPI parsers extract commands, field values, certificates, and device identity - not just port numbers and traffic volume.
- **Evidence-Based Compliance** - Audit-ready evidence generated continuously from observed traffic. No manual evidence collection or periodic assessments.
- **Exposure-Aware Vulnerability Prioritization** - CVEs ranked by real protocol exposure and firmware observations, not theoretical scan results.
- **Air-Gapped & Sovereign Deployment** - Fully on-premises. No cloud dependency. No data leaves the network. Deployed in minutes with a self-extracting installer.
- **No Agents, No Footprint** - Nothing installed on endpoints. Observes from SPAN or TAP ports. Discovers unmanaged and legacy devices that agents cannot reach.
- **Subscription-Based Per-Asset Licensing** - Transparent per-asset pricing that scales with your environment. All platform capabilities, protocol intelligence, and compliance frameworks included in every subscription.

What Customers Gain

- Complete asset inventory - every device, vendor, OS, and firmware version identified from traffic.
- Faster incident investigation - protocol-level evidence for forensic analysis and response.
- OT and medical-device visibility - industrial controllers and clinical devices classified by vendor and model.
- Reduced audit preparation - compliance evidence generated automatically, not collected manually.
- Prioritized remediation - vulnerabilities ranked by observed exposure, not theoretical risk.
- Continuous monitoring - behavioral baselines and threat detection without active probing.
- Legacy device discovery - unmanaged, agentless, and shadow devices visible from wire traffic.
- Operational safety - zero risk of disrupting OT processes, medical devices, or production systems.

Platform Capabilities

Asset Discovery & Classification	Identifies every connected device using multi-signal weighted classification. Vendor, model, OS, firmware, and role assigned automatically from observed protocol behavior.
Protocol Intelligence	Deep packet inspection extracts actual commands, parameters, certificates, and device identity from wire traffic - providing context that port-level tools miss entirely.
Security Insights	Continuously surfaces security findings: cleartext credentials, weak or expired TLS certificates, exposed management interfaces, and unprotected industrial protocols.
Threat & Exposure Analysis	Attack surface scoring, IoC matching from threat intelligence feeds, and per-device behavioral baselines. Detections are deduplicated and actionable.
Vulnerability Prioritization	CVE matching via NVD, CISA KEV, and EPSS. Ranked by observed exposure - which protocols are active, which firmware is running - not by scan-based assumptions.
Medical Device Intelligence	Proprietary clinical protocols parsed by vendor and function. Ventilators, patient monitors, infusion pumps, and analyzers identified from wire-level communication.

Primary Use Cases

- **OT Asset Discovery** - Map every PLC, RTU, HMI, and engineering workstation. Identify cross-zone communication and help enforce segmentation policies.
- **Hospital / IoMT Visibility** - Identify clinical devices by vendor and model. Monitor medical protocol communications across wards and departments.
- **Compliance Evidence Generation** - Auto-generate audit evidence for IEC 62443, ISO 27001, HIPAA, NCA ECC, and NCA OTCC from live traffic observations.
- **Vulnerability & Exposure Prioritization** - Prioritize CVE remediation based on real protocol exposure and active firmware, not theoretical scan outputs.
- **Threat Hunting & IoC Matching** - Match observed network indicators against threat intelligence feeds. Investigate detections with full protocol context.
- **Air-Gapped Network Monitoring** - Deploy fully on-premises with no internet or cloud dependency. Complete functionality in isolated and classified environments.
- **Legacy & Unmanaged Device Visibility** - Discover shadow IT, aging infrastructure, and agentless devices that traditional tools cannot reach or inventory.

Protocol Intelligence

WireTrace includes 250+ deep protocol parsers across industrial, medical, enterprise, and proprietary communications - with continuous expansion. The DPI engine is extensible and designed for ongoing protocol intelligence development.

Industrial / OT	Modbus, S7Comm, EtherNet/IP, PROFINET, BACnet, DNP3, IEC 104, OPC-UA, GOOSE, EtherCAT, HART-IP, FINS, MELSEC, CODESYS, KNXnet/IP, and more+
Healthcare / IoMT	DICOM, HL7, Philips, Draeger, GE CARESCAPE, Hamilton, Masimo, Abbott i-STAT, Capsule DCMP, Welch Allyn, and more+
Enterprise / IT	TLS, SSH, RDP, SMB, DNS, DHCP, LDAP, Kerberos, RADIUS, SNMP,

	HTTP/S, QUIC, WireGuard, OpenVPN, NTP, and more+
IoT / Discovery	SSDP, mDNS, LLDP, CDP, SDDP, NBNS, LLMNR, UPnP, ARP, STP, MPLS, PTP, PPPoE, IGMP, and more+

Representative examples. Protocol library continuously evolves to cover proprietary, vendor-specific, and emerging communications.

Compliance & Audit Evidence

WireTrace generates audit-ready compliance evidence automatically from observed network traffic. This replaces periodic manual assessments with continuous visibility and reduces audit preparation from weeks to hours.

Supported frameworks: IEC 62443 · ISO 27001 · HIPAA · NCA ECC · NCA OTCC · Custom frameworks

Integrations & Ecosystem

- REST API for all data endpoints
- Syslog forwarding and CEF for SIEM integration
- STIX/TAXII threat intelligence exchange
- Webhook notifications and email alerts
- LDAP / Active Directory / OIDC SSO
- CSV export, firewall rule generation (PAN-OS, FortiGate)
- Multi-tenant architecture with role-based access control
- On-premises deployment with full air-gap support

Licensing

WireTrace is licensed per asset on a subscription basis. 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.

- Per-asset subscription pricing
- No module add-ons or feature fragmentation
- All protocol intelligence included
- Continuous platform and protocol updates during subscription
- No cloud dependency required

See WIRETRACE in Your Environment

Request a live demonstration or proof-of-value deployment.
wiretrace.io | sales@wiretrace.io

WIRETRACE