WIRETRACE

SOLUTION BRIEF — ENTERPRISE IT

Complete Network Visibility Without Active Scanning

WireTrace passively discovers every endpoint, server, IoT device, and cloud service on your network. Track TLS certificates, detect cleartext credentials, map your attack surface, and identify shadow IT — all without sending a single packet.

The Challenge

- **Shadow IT and Unknown Devices** — Personal devices, rogue access points, unauthorized servers, and forgotten IoT endpoints connect without IT awareness. Active scanners miss everything in between scans.
- **TLS Certificates Expiring Silently** — Expired, self-signed, and weak TLS certificates expose organizations to attacks and outages. Problems surface only when something breaks.
- **Cloud Services Untracked** — SaaS applications and remote access tools adopted by employees bypass corporate procurement. IT security cannot protect services they do not know exist.
- **Attack Surface Unknown** — Cleartext credentials, exposed management interfaces, weak encryption, and unnecessary services create an attack surface invisible to traditional tools.

How WireTrace Solves It

Passive Asset Discovery	Every device that communicates is discovered automatically. Servers, workstations, printers, phones, IoT devices identified by OS, vendor, model, and function from observed traffic patterns.
TLS Certificate Tracking	Every TLS certificate observed is cataloged: subject, issuer, validity dates, key strength, chain integrity. Self-signed, expiring, and weak cipher suites flagged automatically.
Attack Surface Mapping	Cleartext credentials in HTTP, FTP, SMTP, Telnet detected in real time. Exposed management interfaces, unencrypted database connections, and legacy protocols identified and risk-scored.
Switch Port Identification	LLDP and CDP parsing identifies exactly which switch port each device connects to. Correlate logical identity with physical infrastructure for rapid incident response.

Enterprise Protocol Coverage

TLS · HTTP/S · DNS · DHCP · LLDP · CDP · SNMP · SSH · RDP · SMB · LDAP · Kerberos · RADIUS · NTP · FTP · SMTP · SSDP · mDNS · QUIC · WireGuard · OpenVPN · PostgreSQL · MySQL · Telnet · and more+

Representative examples. WireTrace supports 250+ protocol parsers across enterprise, industrial, medical, and IoT communications, with continuous expansion.

Key Features

Security Insights	Automated security findings from observed traffic. Cleartext credentials, weak TLS, self-signed certificates, exposed admin interfaces, unencrypted database connections surfaced without manual investigation.
Threat & Exposure (Risk Score)	Every asset receives a risk score based on real exposure: observed vulnerabilities, cleartext protocols, certificate issues, open services, behavioral anomalies. Prioritize by actual risk.
Change Management	Track every change: new devices, removed devices, new services, changed configurations, new communication patterns. Full audit trail without relying on CMDB manual updates.
Smart Device Discovery	SSDP and mDNS parsing discovers smart TVs, wireless printers, VoIP phones, smart speakers, and IoT devices that traditional IT tools miss.

Compliance & Governance

WireTrace generates continuous compliance evidence from observed network traffic. Asset inventories, access control validation, encryption posture, and change management documentation are always current.

Supported frameworks: ISO 27001 · NCA ECC · CIS Controls · Custom frameworks

Deployment

A single WireTrace sensor on a SPAN port or TAP captures all enterprise network traffic in a segment. No agents on endpoints, no active scanning, no cloud dependency. Multiple sensors cover campus, data center, and branch office segments with centralized analytics.

First Assets Discovered in Under 30 Seconds

No complex onboarding. No professional services. Deploy the sensor, connect to a SPAN port, and gain complete visibility.
wiretrace.io | sales@wiretrace.io

WIRETRACE