The Business Case for Passive Network Intelligence

WireTrace delivers measurable value across security operations, compliance, incident response, and asset management. This document quantifies the operational and financial impact of deploying passive network intelligence - replacing manual processes, reducing tool sprawl, and accelerating time-to-evidence across IT, OT, IoT, and clinical (IoMT) environments.

80%	90%	70%	1
AUDIT PREP TIME REDUCTION	ASSET INVENTORY ACCURACY GAIN	FASTER INCIDENT INVESTIGATION	PLATFORM REPLACES MULTIPLE TOOLS

VALUE DRIVERS

Eliminate Manual Asset Inventory

Manual walk-through audits, spreadsheet maintenance, and CMDB reconciliation consume hundreds of hours annually. WireTrace replaces manual processes with a continuously updated, traffic-derived inventory that never goes stale.

Reduce Compliance Audit Costs

Preparing for IEC 62443, HIPAA, ISO 27001, and NCA audits typically requires weeks of evidence collection. WireTrace generates audit-ready evidence continuously from observed traffic - reducing preparation time by up to 80%.

Accelerate Incident Investigation

When an incident occurs, investigators need to know which devices communicated, over which protocols, with which commands. WireTrace provides protocol-level forensic evidence immediately - reducing investigation time from days to hours.

Consolidate Visibility Tools

Organizations often run separate tools for IT asset discovery, OT monitoring, vulnerability scanning, and certificate management. WireTrace unifies IT, OT, IoMT, and IoT visibility into a single platform - eliminating tool sprawl and reducing licensing costs.

Prevent Downtime from Active Scanning

Active scanning in OT and clinical environments has caused PLC faults, medical device disconnections, and production outages. WireTrace's passive-by-default architecture eliminates this risk from discovery - the capture interface is receive-only and transmits nothing onto the monitored network, and any optional active enrichment is operator-enabled, scoped, and off by default.

Reduce Mean Time to Detect (MTTD)

Behavioral baselines per device and per protocol detect deviations the moment they occur - unauthorized commands, new communication peers, configuration changes. Continuous monitoring replaces periodic assessments.

COST IMPACT ANALYSIS

CATEGORY	WITHOUT WIRETRACE	WITH WIRETRACE	IMPACT
Annual asset audit labor	400-800 hours	20-40 hours	**95% reduction**
Compliance evidence preparation	4-8 weeks per framework	2-5 days per framework	**80% faster**
Incident investigation time	2-5 days per incident	2-8 hours per incident	**70% faster**
Visibility tool licensing	3-5 separate tools	1 unified platform	**Consolidated**
Active scanning incidents	1-3 disruptions/year	Zero	**Eliminated**
Shadow IT discovery	Periodic / reactive	Continuous / real-time	**Always current**

ROI BY ENVIRONMENT

OT / Industrial

Primary value: Eliminate active scanning risk. Gain visibility into legacy PLCs and RTUs that never appeared in IT inventories. Detect unauthorized programming and cross-zone communications. Generate IEC 62443 and NCA OTCC evidence continuously.

Key metric: Zero active-scanning disruptions. 100% of industrial assets inventoried from traffic.

Healthcare / IoMT

Primary value: Replace manual biomed spreadsheets with a live clinical device inventory. Prove HIPAA segmentation compliance from observed traffic. Identify every ventilator, monitor, and pump by vendor and function.

Key metric: Biomed inventory accuracy from ~40% to 98%+. HIPAA evidence generation continuous.

Enterprise IT

Primary value: Map the real attack surface: expired certificates, cleartext credentials, shadow IT, exposed management interfaces. Prioritize remediation by observed exposure. Track every change on the network automatically.

Key metric: TLS certificate blind spots eliminated. MTTD reduced from days to minutes.

TOTAL COST OF OWNERSHIP ADVANTAGE

No Agent Deployment Overhead

Agent-based platforms require software rollouts to every endpoint - weeks of deployment, ongoing maintenance, compatibility testing, and upgrade cycles. WireTrace requires zero endpoint software. Deploy a sensor in 60 seconds, gain visibility immediately.

No Cloud Subscription

Cloud-dependent platforms carry ongoing SaaS fees, data egress costs, and sovereignty concerns. WireTrace runs entirely on-premises with no cloud dependency. All data stays within the network boundary.

All Capabilities Included

No per-module add-ons. Asset discovery, protocol intelligence, threat detection, compliance evidence, vulnerability prioritization, and behavioral baselines are all included in every subscription. No feature fragmentation.

Rapid Time to Value

First assets classified in under 30 seconds. Full deployment in under 15 minutes. No professional services engagement required. No complex integration project. Value delivered from day one.

RISK REDUCTION SUMMARY

WireTrace reduces organizational risk across multiple dimensions: attack surface visibility (identifying exposures that scans miss), operational safety (eliminating active scanning disruptions), compliance posture (continuous evidence vs. periodic snapshots), and incident response readiness (protocol-level forensic evidence available immediately).

Quantify the Value for Your Environment

Request a proof-of-value deployment to measure WireTrace's impact on your specific asset count, compliance requirements, and operational environment. wiretrace.io | sales@wiretrace.io