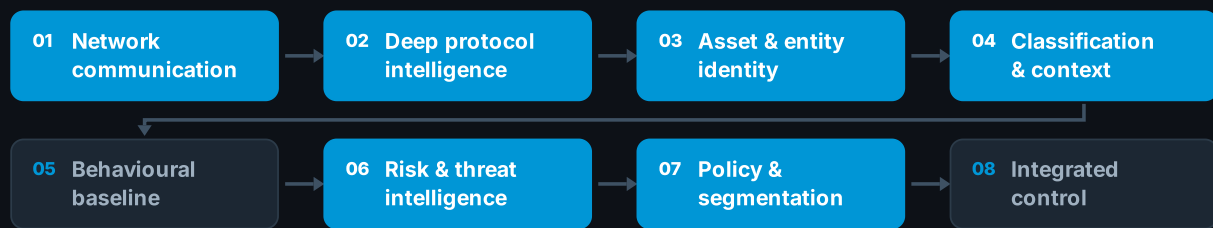


INDUSTRY SOLUTION

Healthcare & IoMT Security

One inventory for medical devices, clinical IT, building systems and IoT, built passively from what each device says on the network, with patient values masked inside the sensor and never stored.



For: Hospital CISOs, biomedical and clinical engineering, healthcare IT and network teams

A hospital network carries imaging modalities, patient monitors, bedside devices and laboratory analysers next to clinical applications, workstations, building management and cameras. Most of the medical devices cannot run an agent, should not be scanned, and are maintained by the manufacturer rather than by IT. **WireTrace understands them from the network communication they already produce, without touching them.**

1

inventory across clinical IT, medical devices (IoMT), building and IoT systems

Masked

patient values masked inside the sensor and never stored

Passive

by default; the capture interface never transmits onto the network

Evidence

for the HIPAA Security Rule and six further frameworks, where the network can show it

01 The challenge in clinical networks

Devices you cannot touch

Regulated, vendor-maintained and sensitive to unexpected traffic: agents are not an option and scanning is a clinical risk.

Devices that move

Monitors and bedside equipment roam between wards and change address, so address-based inventories lose track of them.

Long lives, flat networks

Devices run legacy software for many years and often share segments with systems unrelated to patient care.

02 One inventory, across clinical and non-clinical systems

WireTrace is a **Deep Protocol & Asset Intelligence (DPAI)** platform. Sensors receive mirrored traffic (SPAN, TAP or ERSPAN) and decode protocol payloads, not just headers. Medical devices (IoMT) are discovered and classified alongside clinical IT, building and IoT systems, in one inventory, so the people responsible for each can work from the same picture.

What WireTrace observes

- DICOM, HL7 and a range of medical-device vendor protocols
- Identity records that devices state in their own protocols, and names from DHCP, DNS and directory protocols
- IT protocols such as TLS, SMB, RDP and Kerberos, and building protocols such as BACnet
- Who each device talks to, over which protocols and ports

What it produces

- Devices classified by domain (including medical), device type and role, with a confidence
- One durable identity per physical device, even when it roams and its address changes
- Manufacturer, and model, firmware or serial number where the device states them, each with its source
- A communication map of each device's peers and connection history

Patient data stays out of the platform. For medical protocols, field names are used to understand the device. Patient values are masked inside the sensor and never stored.

For each device, WireTrace also states which kinds of evidence are present, missing or stale, so an unidentified device is never mistaken for a clean one. Devices the evidence cannot classify stay unknown rather than guessed, and become a work list for biomedical engineering.

03 See what puts clinical systems at risk

Exposures

Risks & Exposures brings together clear-text credentials, weak cryptography, exposed services and legacy authentication in one view, with CSV export. Account names and credentials exposed by legacy protocols are detected so weak practices can be fixed; revealing a captured secret is restricted to authorised roles.

Vulnerabilities, where version evidence exists

Each device's identified operating system, software and firmware is matched to the NVD and OT vendor advisories, prioritised with CISA KEV and FIRST EPSS. Every finding states how it was matched and whether the vulnerable version is confirmed on that device. Devices that state no version are not given version-precise findings.

End-of-life technology

Operating systems and products past vendor end of life are flagged, using lifecycle data that also works offline. Coverage depends on what WireTrace can identify; it is not a complete lifecycle record for every medical product.

Ransomware on file shares

Reconnaissance, lateral movement, mass file modification, ransomware extensions and ransom notes on file shares, and unusual exfiltration are correlated into one corroborated verdict, on unencrypted SMB. Encrypted SMB sessions expose no file operations.

Every device receives a 0-100 Asset Risk Score (likelihood × impact) with a separate confidence indicator and a factor breakdown, and the Risk Register ranks devices so remediation, compensating controls or time-limited risk acceptance can be agreed with the clinical owner.

04 Segmentation intent for clinical networks

Separating clinical devices from general IT and building systems is one of the most effective controls a hospital has, and one of the hardest to introduce without disrupting care. WireTrace provides the intelligence, policy intent and continuous validation layer, while your enforcement technologies (firewalls, network access control, switches) execute the network control.

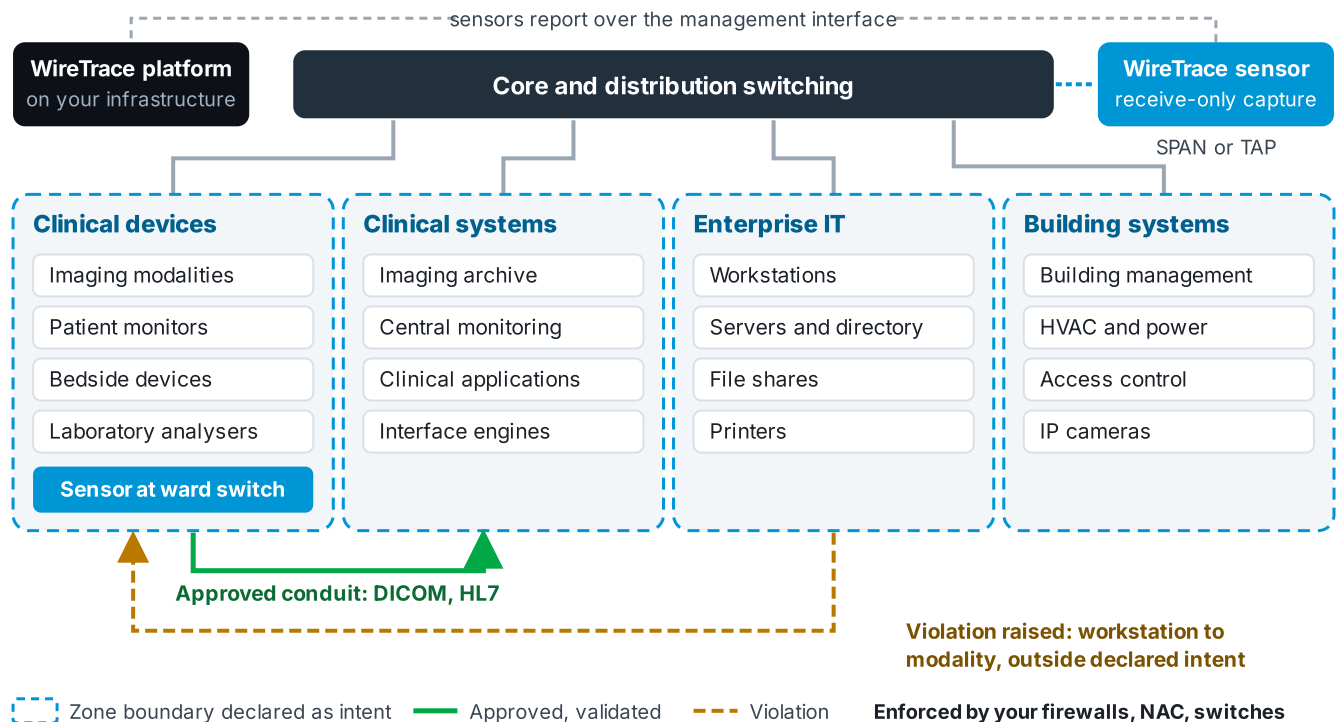


Figure 1. A clinical network as WireTrace sees it. Sensors receive mirrored traffic at the core and at a ward switch. Zones and approved conduits are declared as intent and validated against observed traffic; traffic outside that intent is raised as a violation, and your existing controls enforce the boundaries.

- 1 **Map what depends on what.** The communication map shows which modalities send to which archive, which monitors report to which central station, and which building or IT systems reach clinical devices at all.
- 2 **Baseline and declare intent.** Record a Communication Baseline, approve the expected pairs, and declare which zones and devices may communicate, in which direction and over which services.
- 3 **Validate before change.** Test proposed rules against observed traffic over a bounded window, so a clinical workflow that would be cut is found in review, not on the ward.
- 4 **Hand off and monitor.** Proposed rules are exported as text for your network team, whose firewalls, NAC and switches execute the control. WireTrace then raises traffic that breaks the intent as a violation, with evidence.

05 Compliance evidence, honestly scoped

WireTrace maps network observations to 415 controls across seven frameworks: NIST CSF 2.0, ISO/IEC 27001, HIPAA Security Rule, IEC 62443-3-3, NERC CIP, NCA OTCC and NCA ECC. Every control is rated

observable, partial, manual assessment or not assessable from the network. About a third of controls can be evidenced automatically from the network; auditors close the rest inside the platform's assessment workflow. For the HIPAA Security Rule, that means network evidence where the network can show it, and a place to record the evidence it cannot. Compliance evidence can be exported as a signed evidence bundle.

06 Safe by design for clinical environments

Passive by default

The capture interface only receives; it never transmits onto the monitored network. Nothing is installed on the devices being observed.

Optional enrichment, kept away from medical devices

Administrators can add read-only switch polling and credentialed collection for IT systems, within scopes they define. The OT-safe profile keeps active probes away from industrial and medical devices unless an administrator explicitly allows them.

On your infrastructure

WireTrace installs on servers or virtual machines you own, and analysis runs there. It can operate fully without internet access.

Fits existing operations

Alerts reach your SIEM over syslog or the Splunk HTTP Event Collector, and a read-only REST API exposes assets, risk and alerts to the tools you already run.

Limits, stated plainly

- WireTrace sees what reaches its sensors. Wards, departments and remote sites need sensor coverage or mirrored traffic to be included.
- Model, firmware and serial number are recorded where devices state them. Many medical devices do not reveal them passively, and vulnerability findings follow the version evidence available.
- WireTrace does not decrypt traffic. Encrypted sessions yield identity, certificate and behavioural evidence, not content; ransomware file-activity detection works on unencrypted SMB.
- WireTrace defines, validates and monitors segmentation intent. Your firewalls, NAC and switches enforce it.
- Compliance mapping provides network evidence; it does not make an organisation compliant. Controls that the network cannot show are assessed by people, inside the platform.

Start with one clinical network

A WireTrace evaluation listens passively on a mirrored port in front of one ward, imaging department or clinical data centre, and shows what is there without touching a single device.

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