TECHNICAL DOCUMENTATION

# For this workload, this is the hardware we recommend.

This guide tells you what to provision for the two parts of a WireTrace deployment: the **sensor** that receives mirrored traffic, sized by monitored traffic level, and the **platform** that turns its observations into asset intelligence, sized by asset count and retention. The recommendations are conservative and ready to build a bill of materials from.

Figures assume a **mixed enterprise traffic profile** and apply to WireTrace release 1.3.6 and later. Environments with unusually high packet rates, such as dense small-frame industrial telemetry, may require workload-specific sizing, which WireTrace performs with you during solution design.

## RECOMMENDED SENSOR HARDWARE

| MONITORED TRAFFIC | RECOMMENDED CPU | RAM | DISK | MONITORING NIC |
|---|---|---|---|---|
| **500 Mbps** | **2 physical cores** | 8 GB | 40 GB | 1 GbE |
| **1 Gbps** | **4 physical cores** | 8 GB | 80 GB | 10 GbE |
| **5 Gbps** | **24 physical cores** | 16 GB | 250 GB | 10 GbE |
| **10 Gbps** | **64 physical cores** | 32 GB | 500 GB | 25 GbE |

CPU is stated in physical cores, not vCPUs or hardware threads: see virtual deployment on page 2. Each sensor also requires a separate 1 GbE management interface. Minimum supported host is 2 physical cores, 4 GB RAM and 10 GB free disk; the installer will not proceed below these. Sensor disk is used for temporary buffering during platform connectivity interruptions and holds no long-term data; use SSD storage at 5 Gbps and above.

**How these recommendations are derived.** Recommended capacities are based on controlled validation testing on production-class hardware, with operational headroom included. High-throughput deployments are additionally validated against the customer's actual traffic profile during solution design, so the configuration you commit to reflects your network, not a nominal figure.

**Larger and distributed environments.** Multi-site and geographically distributed deployments typically run one sensor per site or capture point, all reporting to a single platform and deduplicating into one estate-wide asset inventory. WireTrace sizes multi-sensor architectures with you during solution design.

## VIRTUAL DEPLOYMENT

**Size virtual sensors on physical cores, not vCPUs.** A 16 vCPU virtual machine backed by 8 physical cores is an 8-core sensor and must be sized as one. On any SMT-enabled host, assume 2 vCPU per physical core. Sensor processing configuration is managed automatically by WireTrace.

| SENSOR CONFIGURATION | VCPU ON AN SMT HOST | UNDERLYING PHYSICAL CORES | RAM | DISK |
|---|---|---|---|---|
| **2-core** (500 Mbps) | 4 | 2 | 8 GB | 40 GB |
| **4-core** (1 Gbps) | 8 | 4 | 8 GB | 80 GB |

The 24-core and 64-core configurations should be deployed on physical hosts, and mirror delivery at those rates depends on passthrough NIC access in any case.

**Reserve the CPU**
Reserve the sensor's vCPUs in the hypervisor. A sensor sharing oversubscribed cores will drop packets under burst regardless of its sizing. Do not hot-add CPU after deployment.

**Pass the mirror through cleanly**
Deliver the monitoring feed by SR-IOV or PCI passthrough above roughly 300 Mbps. Paravirtual adapters add per-packet cost in the hypervisor that the sensor cannot recover. Promiscuous mode must be permitted on the port group carrying the mirror.

## CAPTURE REQUIREMENTS

| REQUIREMENT | SPECIFICATION |
|---|---|
| **Capture sources** | Switch SPAN / mirror port, network TAP, ERSPAN, 802.1ah PBB mirror. Encapsulated mirrors are decapsulated and the inner frame is analysed. |
| **Interfaces** | Minimum two: one dedicated monitoring interface with no IP address, in promiscuous mode, receive only; one management interface. |
| **Mirror capacity** | The mirror source must deliver the full monitored traffic without oversubscription: a mirror port that drops frames drops them invisibly, before the sensor can account for them. Prefer TAPs or dedicated SPAN sessions at higher rates. |
| **Frame size** | Set the capture MTU to accommodate encapsulation overhead, typically 1,600 B for ERSPAN. |
| **NIC selection** | Use a server-class monitoring NIC matching the table on page 1. WireTrace confirms the capture configuration for the 24-core and larger configurations during solution design. |

## PLATFORM SIZING

The platform runs analytics, classification, threat detection, compliance evidence and the interface, and holds all data. Its size is driven by monitored asset count and retention period, shaped by protocol mix and the aggregate workload of the connected sensors.

| PROFILE | MONITORED ASSETS | CPU | RAM | DISK | RETENTION | TYPICAL ENVIRONMENT |
|---|---|---|---|---|---|---|
| **Small** | Up to 500 | 4 vCPU | 16 GB | 200 GB SSD | 90 days | Single OT site, small hospital wing, branch office |
| **Medium** | 500 – 2,000 | 8 vCPU | 32 GB | 500 GB SSD | 180 days | Manufacturing plant, mid-size hospital, campus network |
| **Large** | 2,000 – 10,000 | 16 vCPU | 64 GB | 1 TB SSD | 365 days | Multi-building campus, large hospital, utility SCADA |
| **Enterprise** | 10,000 – 50,000 | 32 vCPU | 128 GB | 2 TB NVMe | 365+ days | Multi-site enterprise, large utility, national infrastructure |

SSD is required at every profile; NVMe is required at Enterprise and recommended at Large. Add 2 GB RAM and one core where AI report generation is enabled.

**Size the platform for the workload, not the asset count alone.** A deployment that monitors high traffic relative to its asset count needs the platform sized for the traffic. If in doubt between two profiles, take the larger. 5 and 10 Gbps deployments, and any Enterprise-profile deployment, receive a workload-specific platform sizing during solution design so the platform matches the sensors feeding it.

## PLATFORM STORAGE AND RETENTION

WireTrace stores parsed protocol fields and derived intelligence, not full packet captures, so storage follows asset count and protocol mix rather than raw bandwidth. The estimates below assume typical mixed OT/IT protocol distributions; environments heavy in high-volume protocols such as DNS and HTTP trend toward the top of each range.

| ASSETS | 90-DAY RETENTION | 180-DAY RETENTION | 365-DAY RETENTION |
|---|---|---|---|
| 500 | 40 – 80 GB | 80 – 150 GB | 150 – 300 GB |
| 2,000 | 100 – 200 GB | 200 – 400 GB | 400 – 750 GB |
| 10,000 | 300 – 500 GB | 500 GB – 1 TB | 1 – 2 TB |
| 50,000 | 500 GB – 1 TB | 1 – 2 TB | 2 – 4 TB |

## OPERATING SYSTEM AND VIRTUALISATION

| REQUIREMENT | SUPPORTED OPTIONS |
|---|---|
| **Platform and sensor OS** | Ubuntu Server LTS x86_64: 22.04, 24.04, 26.04 |
| **Virtualisation** | VMware ESXi 7.0+, KVM/QEMU, Microsoft Hyper-V, Proxmox VE, Oracle VirtualBox |
| **Physical deployment** | Any x86_64 hardware meeting the sizing tables in this guide |
| **Container runtime** | Installed automatically by the WireTrace installer if not present |
| **Time synchronisation** | NTP or chrony on the platform and all sensors |

## NETWORK REQUIREMENTS

| PATH | DETAILS |
|---|---|
| **Web UI access** | HTTPS (443/TCP) from management workstations to the platform; 80/TCP for redirect only |
| **Sensor to platform** | TCP on the configured transport port (default 6379) for observations; HTTPS (443/TCP) for configuration and log shipping. Typically 1–10 Mbps per sensor. |
| **Optional ingest** | Syslog 514/UDP and 514/TCP; SNMP traps 162/UDP |
| **Internet** | Not required. All features operate fully air-gapped. Optional access enables NVD/CVE feed updates. |
| **DNS** | Optional. Used for NVD feed resolution and OIDC SSO if configured; not required for core functionality. |

## DEPLOYMENT CHECKLIST

**Platform**

- VM or physical host provisioned per sizing profile
- Ubuntu Server LTS installed, SSH access for the installer
- SSD storage mounted (NVMe for Enterprise)
- Network connectivity to every sensor host
- HTTPS (443) reachable from the management network

**Sensor (per unit)**

- Host provisioned per the sizing table, **physical cores confirmed**
- Capture NIC on SPAN/TAP, promiscuous, no IP address
- Mirror source able to deliver the monitored traffic in full
- Management NIC with connectivity to the platform; activation token from the platform
- No internet required: sensors operate fully offline

### Want this worked through against your diagram?

Bring a network diagram and, if you have them, packet counters from the switches you would mirror. In one session we will place the mirror points, size the sensors against your real traffic, and confirm the platform profile, including the workload check most sizing exercises skip.

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