Deployment & Sizing Guide

WireTrace is designed for lightweight deployment across environments of all sizes — from a single OT network segment to enterprise-wide multi-site installations. This guide provides infrastructure sizing recommendations based on environment scale, monitored bandwidth, and data retention requirements.

Server Sizing

The WireTrace Server runs the analytics engine, classification pipeline, threat detection, compliance evidence generation, web interface, and all data stores.

Profile	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
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 infra

Sensor Sizing

Each DPI Sensor captures and parses traffic from a SPAN port or network TAP. Sensors are lightweight by design.

Profile	Bandwidth	CPU	RAM	Disk	Typical Environment
Standard	Up to 200 Mbps	4 vCPU	8 GB	40 GB	OT segment, clinical VLAN, branch office
Enhanced	200 Mbps-1 Gbps	8 vCPU	16 GB	80 GB	Campus core, data center segment
High-Throughput	1-5 Gbps	16 vCPU	32 GB	160 GB	Internet edge, aggregation layer
Ultra	5-10 Gbps	32 vCPU	64 GB	200 GB	Core backbone, 10G TAP, high-density DC

Deployment Profiles

Single-Site OT (Small Server + 1 Sensor)	One OT network, single SPAN port. 4 vCPU/16 GB server + 4 vCPU/8 GB sensor. Deployed in under 15 minutes.
Hospital / Clinical (Medium Server + 2-4 Sensors)	Multiple clinical VLANs. One sensor per segment. 8 vCPU/32 GB server + 2-4 Standard sensors.
Campus / Multi-Building (Large Server + 4-8 Sensors)	OT, IT, IoT segments. Mix of Standard/Enhanced sensors. 16 vCPU/64 GB server.
Enterprise / Multi-Site (Enterprise Server + 10+ Sensors)	Multiple locations, centralized server. 32 vCPU/128 GB server. Year-long retention.

Operating System & Virtualization

- Server/Sensor OS: Ubuntu 22.04 LTS, Ubuntu 24.04 LTS
- Virtualization: VMware ESXi 7.0+, KVM/QEMU, Microsoft Hyper-V, Proxmox VE, Oracle VirtualBox
- Container Runtime: Docker Engine 24+ with Compose V2 (pre-installed by WireTrace installer if not present)
- Physical: Supported on any x86_64 hardware meeting sizing requirements

Network Requirements

- Sensor capture interface: Dedicated NIC on SPAN/TAP. Promiscuous mode. No IP assigned.
- Sensor management interface: Separate NIC with TCP connectivity to server (default port 6379).
- Web UI: HTTPS (port 443) from management workstations to server.
- Internet: Not required. All features operate fully air-gapped. Optional for NVD/CVE feed updates.

Storage & Retention Guidance

Estimates assume typical mixed OT/IT protocol distributions. Environments with predominantly high-volume protocols (DNS, HTTP) trend toward the higher end. WireTrace stores parsed protocol fields, not full PCAPs.

Assets	90-Day	180-Day	365-Day
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

Deployment Checklist

Server:

- VM or physical host provisioned per sizing profile
- Ubuntu 22.04 or 24.04 LTS installed
- SSH access for installer execution
- SSD storage (NVMe for Large/Enterprise)
- Network connectivity to all sensor hosts
- HTTPS port (443) accessible from management network

Sensor (per unit):

- VM or physical host per sensor profile
- Ubuntu 22.04 or 24.04 LTS installed
- Capture NIC connected to SPAN/TAP (promiscuous mode)
- Management NIC with connectivity to server
- Activation token from WireTrace Server
- No internet required — fully offline operation

Need Help Sizing Your Deployment?

Contact the WireTrace team for a customized recommendation.
sales@wiretrace.io