WIRETRACE

TECHNICAL ARCHITECTURE OVERVIEW

Platform Architecture Overview

WireTrace is a distributed sensor-server architecture designed for passive network intelligence. Sensors capture and parse traffic at the wire level; the server performs classification, analytics, threat detection, and compliance evidence generation. Fully on-premises. Air-gap deployable. No cloud dependency.

Data Flow

SPAN/TAP --> DPI Sensor (native engine, 250+ parsers) --> Encrypted Stream Transport (structured JSON) --> Analytics Server (classification, threat detection, compliance) --> Web UI / REST API

Core Components

DPI Sensor	High-performance native deep packet inspection engine optimized for real-time protocol analysis. Captures from SPAN/TAP, parses 250+ protocols, outputs structured JSON. Cryptographically signed payloads. Zero packets transmitted on monitored network. Deployed in under 60 seconds.
Analytics Server	Centralized intelligence engine. Multi-signal weighted classification, behavioral baselines, CVE matching (NVD, CISA KEV, EPSS), IoC matching (STIX/TAXII), compliance evidence generation. Multi-tenant with RBAC. Real-time notifications.

Data Stores

Relational Database	Primary structured store for asset inventory, connection state, classification history, security observations, threat detections, compliance evidence, and tenant configuration.
In-Memory Stream & Cache	High-throughput stream transport for the sensor-to-server data pipeline. In-memory caching for dashboard queries and API response acceleration.
Object Store	S3-compatible local storage for raw parsed data, protocol captures, and generated reports. Runs entirely on-premises - no external cloud dependency.

Deployment Models

- **Single-Site** - One server, one or more sensors. All Docker containers via Docker Compose. Self-extracting .run installer in under 10 minutes. No internet required.
- **Multi-Site / Distributed** - Remote sensors connect to centralized server. Independent operation during interruptions, sync on reconnect. Supports segmented OT, campus, branch topologies.

Security Architecture

- **Transport Security** - Sensor-to-server cryptographically signed. Per-sensor unique secret. Activation token enrollment. TLS for all API/UI.
- **Platform Security** - Asymmetric cryptography license validation. JWT authentication with RSA key pairs. RBAC. Multi-tenant data isolation. LDAP/AD/OIDC SSO. CSRF protection.

Protocol Intelligence Engine

The DPI sensor parses protocols at the application layer, extracting structured fields specific to each protocol. Full payload dissection with protocol-aware field extraction - not signature matching or port-based identification.

Industrial / OT	Modbus function codes, S7Comm PLC parameters, DNP3 control commands, EtherNet/IP CIP, IEC 104, OPC-UA, PROFINET, BACnet, GOOSE, and more+
Healthcare / IoMT	DICOM imaging, HL7 clinical messaging, Philips Respironics, Draeger, GE CARESCAPE, Hamilton, Masimo, Abbott i-STAT, and more+
Enterprise / IT / IoT	TLS certificate extraction, DNS, DHCP, LLDP/CDP switch port mapping, SSDP/mDNS, SMB, SSH, RDP, and more+

Integration Points

REST API (all endpoints) · Syslog Forwarding · CEF / SIEM · STIX / TAXII · Webhooks · Email Alerts · CSV Export · Firewall Rules (PAN-OS, FortiGate) · LDAP / AD / OIDC SSO

Supported Environments

- Operating System: Ubuntu 22.04 LTS and 24.04 LTS
- Virtualization: VMware ESXi, KVM/QEMU, Hyper-V, Proxmox. Physical or virtual deployments supported.
- Network: Passive capture from SPAN port or network TAP. No inline deployment. Air-gap supported.

For detailed infrastructure sizing by environment size (assets, bandwidth, retention), refer to the WireTrace Deployment & Sizing Guide.