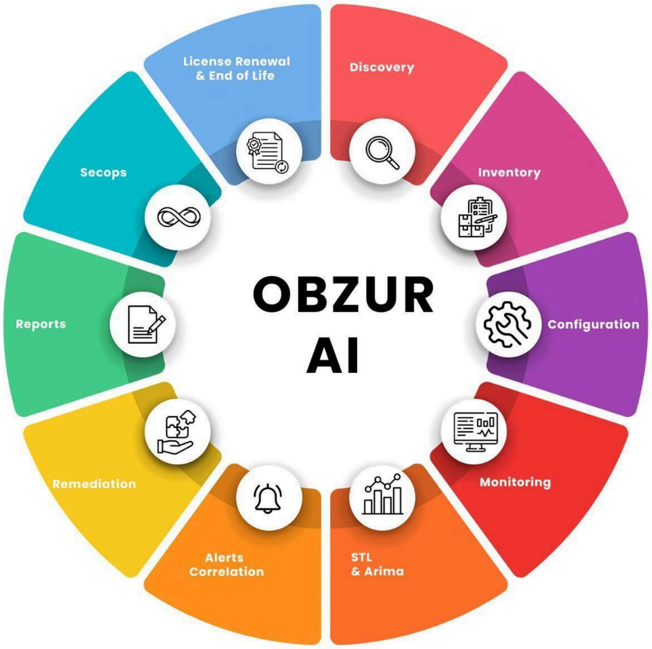
ObzurAI

ObzurAI is a unified AI-driven observability and security intelligence platform designed to manage the complete lifecycle of IT and IoT resources across Private Cloud, Public Cloud, Data Centers, and Edge locations.

From Discovery to Decommissioning, from Server to Camera, from Alert to Auto-Remediation — ObzurAI delivers one single command center for infrastructure, applications and video intelligence.

LIFE CYCLE



Discover

Obzur AI automatically discovers IT and IoT assets across networks, branches, and clouds.This ensures no device is left unmonitored.

Inventory

Each discovered asset becomes part of a unified inventory – with type, location, owner and criticality – so you know *what* is being monitored and *where* it lives.

Configuration

Monitoring starts with the right configuration. Obzur AI learns device roles and suggests monitoring profiles: what metrics to collect, what thresholds to start with, and how to group similar assets.

Monitor

Obzur AI continuously collects metrics, logs and events from IT and IoT devices. It also monitors video surveillance systems. Monitoring dashboards show real-time health, performance and availability.

Smart Surveillance

ObzurAI includes Smart Surveillance, an AI-powered video intelligence layer.

STL & Arima

Using Seasonal Pattern and Trend, Obzur AI understands how assets behave over time – business hours vs off-hours, weekdays vs weekends, seasonal peaks – and detects abnormal behaviour based on real patterns.

Alerts Correlation

ObzurAI delivers clean, meaningful alerts by automatically correlating related events to identify the true root cause. Instead of showing scattered signals, the platform groups alert chains, highlights dependency impact, and filters out noise—ensuring teams see only high-priority, actionable alerts.

Remedies

For important incidents, Obzur AI suggests context-aware remedies – from quick checks to detailed runbooks and automation steps. Operators can move faster from *“we see the problem”* to *“we know what to do next”*.

Reports

Generates scheduled or on-demand reports covering assets, alerts, and remediation actions.

SecOps

ObzurAI produces **comprehensive security reports** that clear visibility into potential risks and help teams prioritize remediation based on impact.

License Renewal and End of the Life

Obzur AI tracks license status, support timelines and end-of-life dates for assets across your environment. This lifecycle awareness helps you plan renewals, upgrades and safe decommissioning, reducing risk from outdated or unsupported IT and IoT devices.

Smart Alert System

Obzur AI makes alerts simple, accurate, and noise-free. The platform uses Alert Correlation to group alert chains and find the real root cause instead of showing alerts as separate signals. With Alert Correlation Ratio, it measures how one alert affects another and shows device dependency impact clearly. To stop alert overload, Alert Ratio Analysis filters noise and keeps only high-impact alerts that truly need attention. Once a real issue is detected, an alert is raised instantly, followed by automated Ticket Generation that creates the corresponding detailed, incident ticket for fast and structured response.

Adaptive Threshold Algorithm

Traditional monitoring relies on manual and hardcoded thresholds. Ozbur AI replace with adaptive,intelligent thresholds what truly matters:

- **STL (Seasonal-Trend decomposition using Loess):** STL separates time-series data into three components — Trend, Seasonality, and Residual noise — to understand recurring behavior in devices .

  It helps the system recognize daily, weekly, monthly, or seasonal usage patterns, making alerts more adaptive by comparing the current behavior with its *expected* seasonal pattern rather than a fixed threshold.
- **ARIMA:** It learns from the Loess-smoothed residual and predicts future residual points.

SecOps

ObzurAI strengthens security with an integrated SBOM-driven vulnerability intelligence engine. The platform continuously analyzes applications, firmware, and dependencies to generate detailed Software Bills of Materials (SBOMs). Each component is automatically matched against global CVE databases to identify vulnerabilities, supply-chain risks, and outdated or risky libraries.

ObzurAI produces **comprehensive security reports** that clear visibility into potential risks and help teams prioritize remediation based on impact.

With recommendations for patches, safer dependency versions, and compliance-ready summaries, SecOps becomes a built-in security layer across the entire device lifecycle.

Smart Surveillance

ObzurAI includes Smart Surveillance, an AI-powered video intelligence layer.

Traditional Surveillance:

- Trigger every motion
- No learning
- No intelligence

Smart Surveillance:

- Learns daily patterns
- Understands behavior
- Identifies abnormal events

Industry Use-Cases

1. Hospital – 🏥
2. Supermarket – 🛒
3. Railway Station – 🚉
4. Bank – 🏦
5. IT Companies – 💻 / 🖥️
6. Hotels & Hospitality – 🏨
7. Manufacturing Plants – 🏭
8. Educational Institutions – 🏫
9. Data Centers – 🗄️
10. Airports – ✈️