Obzora.

Network Monitoring Solution

Compliant Surveillance & Infrastructure Monitoring Platform

Unified Monitoring for CCTV, NVR/DVR, VMS, Switches, Servers, UPS, and Storage Systems

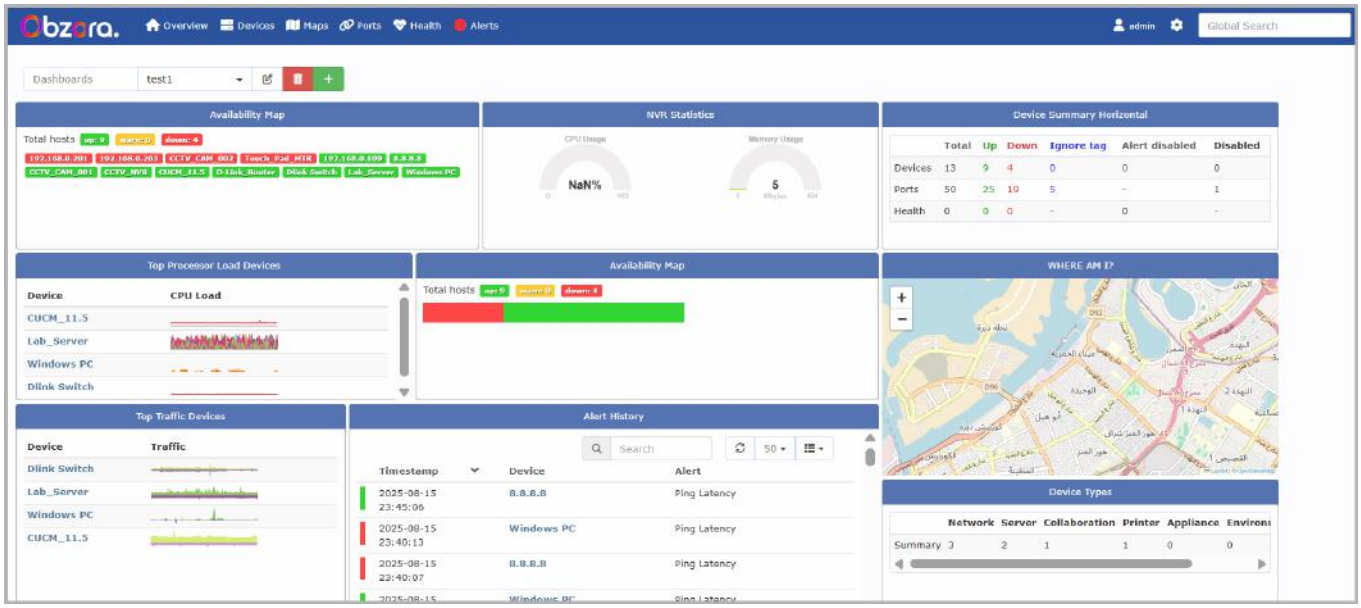
Executive Summary

Obzora NMS is a unified monitoring platform that delivers complete oversight of surveillance and IT infrastructure. It seamlessly integrates with CCTV cameras, NVRs, Video Management Systems (VMS), network switches, servers, and other critical devices to ensure continuous performance and security. By providing real-time status, performance metrics, and alerts. Obzora NMS enables proactive maintenance, reduces downtime, and ensures smooth operation of both security and network systems. Its compliance-ready architecture supports industry standards, making it the ideal choice for organizations that require reliable surveillance and infrastructure monitoring.

In United Arab Emirates, security and surveillance infrastructure is governed by stringent operational standards set by the Security Industry Regulatory Agency (SIRA). These standards ensure that systems remain reliable, resilient, secure and continuously operational.

As per Security Industry Regulatory Agency (SIRA) **Administrative Resolution No. (13) of 2025**, "The network must be equipped with a network management system (NMS). This system must include all means of monitoring network operation, identifying outages, and automatically reporting them if the number of devices connected to the network exceeds 200 devices."
Referral link: http://obzora.net/sira.html (Chapter One: Digital Systems Specifications (IP) -> Fifth: Network)

Obzora is specifically designed to fulfill SIRA compliance requirements for surveillance infrastructure. Unlike generic monitoring tools, it is tailored for security device health monitoring — covering CCTV cameras, NVR/DVR units, VMS platforms, switches, servers, UPS units, and storage systems.
By combining predictive analytics, proactive alerts, and a vendor-neutral architecture, Obzora empowers security integrators, facility managers, and government authorities to maintain uninterrupted surveillance coverage and remain audit-ready at all times.



Background

The operational integrity of a surveillance system is only as strong as its weakest component. A failed hard drive in an NVR, a malfunctioning UPS, or a network switch outage can lead to partial or total loss of video evidence — potentially compromising safety and compliance.

With the diversity of hardware in modern security ecosystems — often sourced from multiple vendors — the need for a **centralized, brand-agnostic monitoring** solution is critical.

Challenges in Surveillance Monitoring

- **Device Diversity:** Different brands, models, and firmware versions create integration complexity.
- **Reactive Maintenance:** Failures are often detected only after critical downtime.
- **Compliance Burden:** Manual record-keeping is error-prone and time-consuming.
- **Scalability:** Many tools fail to handle large-scale deployments efficiently.

Purpose of Obzora

- Offering comprehensive, continuous monitoring for all surveillance-related devices.
- Providing predictive fault detection to prevent outages before they occur.
- Maintaining compliance-ready records for SIRA audits.
- Supporting seamless integration with devices from multiple vendors.

SIRA Compliance Mapping

SIRA Compliance Requirement	Obzora Capability	Compliance Mechanism
Real-time monitoring of all security devices	Multi-vendor monitoring engine	SNMP, ICMP, API, Syslog
Immediate detection of device failures	Intelligent alert engine	Configurable thresholds & escalation
Device uptime and event logging	Historical data retention	SQL database with export tools
Storage health monitoring	HDD SMART checks & utilization alerts	Prevents recording loss
UPS and power source monitoring	Voltage, load, battery status tracking	SNMP-based power monitoring
Secure system access	Multi-Factor Authentication (MFA)	Role-based access control
Automatic reporting if devices exceed 200	Provides automated notifications once the device count surpasses 200.	Clustered deployment
Automated compliance reports	Scheduled PDF/CSV/XLS generation	Audit-ready documentation
Encrypted communications	HTTPS/TLS protocols	Secure credential handling

(Note: Each point aligns directly with the current SIRA regulatory framework for CCTV system monitoring.)

Key Features

- Real-time alerts and notifications
- Centralized dashboard for monitoring and reporting
- Scalable architecture supporting 1000+ devices per instance

Multi-Vendor Device Monitoring

- Integrates seamlessly with CCTV, NVR, DVR, VMS, Switch, Servers, UPS & Storage devices from multiple vendors, eliminating compatibility issues
- Communicates through SNMP, ICMP, HTTP(S), and Syslog protocols for real-time monitoring
- Provides a unified dashboard for all devices, regardless of brand
- Supports both on-premises and distributed sites
- Maintains a centralized inventory with automatic device discovery
- Monitors and alerts when the total device count in the network reaches a defined threshold

CCTV & Video Device Health Tracking

- Monitors camera connectivity and video stream availability
- Tracks NVR/DVR recording status
- Logs and alerts on camera disconnections or recording stoppages
- Ensures uninterrupted video coverage to meet SIRA uptime requirements

Storage & HDD Health Monitoring

- Monitors available storage capacity
- Detects early signs of disk failure via SMART diagnostics
- Sends pre-emptive alerts for abnormal disk temperature, read/write errors, and degraded RAID arrays
- Prevents loss of recorded footage by enabling timely maintenance

UPS & Power Monitoring

- Tracks battery charge levels, load percentage, and voltage status
- Issues alerts for power failures or critically low battery conditions
- Ensures uninterrupted recording during power outages

Server & Network Performance Monitoring

- Monitors CPU, RAM, bandwidth usage, and network latency
- Detects switch port failures or misconfigurations
- Identifies unusual traffic spikes that may indicate network problems

Multi-Factor Authentication (MFA)

- Restricts platform access to authorized personnel only
- Reduces risk of unauthorized changes or data breaches
- Role-based access control

Intelligent Alerts & Notifications

- Real-time alerts and notifications
- Configures alerts for disk space usage thresholds
- Sets alerts for CPU or memory overload
- Triggers alerts for device disconnections
- Sends notifications via email, SMS, third-party API's and web dashboard
- Generate Tickets and notify in Social apps (Telegram, WhatsApp, etc.) for instant updates.

Historical Reporting & Audit Logs

- Supports automatic report scheduling (daily, weekly, monthly)
- Exports reports in PDF, CSV, or XLS format
- Stores event logs for extended compliance and auditing purposes

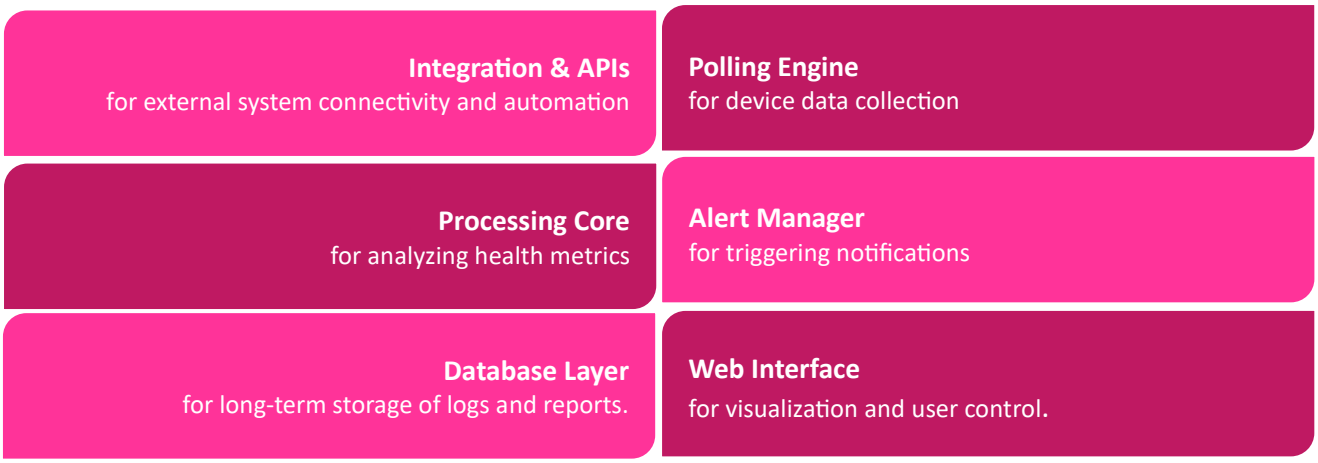
Deployment Options

On-Premises virtual machine
For organizations with strict data control requirements.

Private Cloud
Secure access from multiple remote sites via VPN.

Pre-Configured Hardware
For quick installation and seamless integration with existing networks

Architecture Overview



Security & Data Protection

Feature	Description
MFA (Multi-Factor Authentication)	Adds an extra layer of login security to prevent unauthorized access.
Role-Based Access Control	Users can access only what is assigned to their role, ensuring data security and compliance.
Encryption	Data in transit and stored credentials are encrypted for confidentiality.
Secure Storage of Credentials	Device login credentials are stored securely within the system.

Device Compatibility Matrix

Category	Vendor	SNMP Supported	Monitoring in ObzoraNMS	Remarks
Switches (PoE/Non-PoE)	Cisco (Catalyst, Nexus, Small Business series), HP Aruba, D-Link, TP-Link Switch / JetStream, Huawei, Ruijie, Arista (EOS, MOS), ZyXEL Ethernet Switch	☑ Yes	Ports, PoE, VLAN, CPU/Memory	Feature depth varies by vendor
Routers/Firewalls	Cisco, Fortinet, Huawei, Palo Alto, Mikrotik, SonicWall, Sophos, Juniper, Huawei, WatchGuard, SonicWall	☑ Yes	Interfaces, CPU/Memory, Routing Protocols	Feature depth varies by vendor
CCTV Cameras (IP)	Hikvision, Dahua, Axis, Bosch, Hanwha Techwin, Uniview, CP Plus, Vivotek, Illustra, Grandstream, Honeywell, IMOU	⚠ Limited	Uptime, Availability, Bandwidth	Feature depth varies by vendor
Analog DVR	Hikvision, Dahua, CP Plus, Honeywell, Swann, Lorex	⚠ Limited	Limited monitoring	SNMP limited; integration via vendor API
NVR	Hikvision, Dahua, Uniview, Honeywell, Bosch, Hanwha Techwin, Grandstream, IMOU	☑ Yes	Basic System Info, Storage, Network	SNMP supported; integration via vendor API
VMS (Video Mgmt)	Milestone, Genetec, NUUO, Avigilon, Digifort, Hanwha Wisenet WAVE, Uniview EZVMS/UniVMS, CP Plus VMS, Vivotek VAST2, Illustra VMS, Honeywell MAXPRO, Imou Studio/Imou Life	⚠ Limited	API/Trap-based	SNMP limited; integration via vendor API
Servers	Dell, HP, Lenovo, Supermicro, Huawei, Cisco UCS, Fujitsu, IBM, Inspur, Oracle	☑ Yes	CPU, Memory, Disk, Fans, PSU	OS level SNMP
Storage (NAS/SAN)	Dell EMC, HPE, NetApp, Synology, QNAP, Huawei, Hitachi Vantara, IBM Storage, Lenovo, Supermicro , QNAP, NetApp	☑ Yes	CPU, Memory, Disk, RAID, Fans, PSU	Feature depth varies by vendor
UPS/Power	APC, Eaton, Vertiv, Riello, Socomec, Delta, Schneider Electric, Huawei	☑ Yes	Load, Battery, Runtime, Alarms, Input/output voltage	Feature depth varies by vendor

PDU (Power Distribution)	APC, Eaton, Raritan, Vertiv, CyberPower, Schneider Electric, Tripp Lite	☑ Yes	Outlet status, load monitoring	Requires SNMP-enabled models
Access Control	Honeywell, HID, ZKTeco, Suprema, Bosch, Gallagher, Johnson Controls (C-CURE), Anviz, LenelS2, Vanderbilt, Soyal	⚠ Limited	Limited via API	Feature depth varies by vendor
Biometric Devices	Suprema, ZKTeco, HID, Dermalog, Morpho (IDEMIA), Anviz, Secugen, Nitgen, Soyal, Realand	⚠ Limited	Limited monitoring	Most expose APIs, not SNMP
Environmental Sensors	AKCP, Avtech, HW group	☑ Yes	Temperature, Humidity, Alarms	SNMP-based sensors supported
Wireless APs & Controllers	Cisco, Ubiquiti, Aruba, TP-Link, Ruckus, MikroTik, Cambium Networks	☑ Yes	Clients, Traffic, Signal	Depends on vendor MIBs

ObzoraNMS – System Requirements

Deployment Size	CPU	RAM	Storage	Network
Small (≤500 devices)	2 cores (2 GHz+)	8 GB	1 TB (HDD/SSD)	2 x 1 Gbps NIC
Medium (500–2,000 devices)	4–8 cores	16–32 GB	1 TB – 4 TB (SSD/NVMe)	2 x 1–10 Gbps NIC
Large (2,000+ devices)	16+ cores	64+ GB	4 TB+ (SSD/NVMe)	2 x 10 Gbps+ NIC

Recommendations

- Deploy on **SSD/NVMe** storage for optimal performance.
- Use **dedicated monitoring servers** for large CCTV/enterprise environments.
- Keep ObzoraNMS & OS **regularly updated** for security & stability.

ObzoraNMS – Example Use Cases

Commercial & Enterprise

Airports – Multi-terminal Surveillance Monitoring

Challenge: Thousands of IP cameras and PoE switches spread across terminals need continuous uptime.
Solution: Real-time device health checks, camera disconnect alerts, bandwidth monitoring per terminal.
Benefit: Ensures uninterrupted surveillance and faster fault isolation.

Shopping Malls – Storage & Recording Protection

Challenge: HDD/RAID failures in NVRs can lead to recording loss.
Solution: Proactive monitoring of storage utilization, RAID health, and disk failures.
Benefit: Prevents recording gaps, ensuring reliable video evidence.

Data Centers – Infrastructure & Power Monitoring

Challenge: Critical UPS, servers, and cooling systems require round-the-clock visibility.
Solution: UPS runtime/battery monitoring, server CPU/memory utilization, temperature & humidity sensors.
Benefit: Maximizes uptime and prevents costly outages.

Banks & Financial Institutions – Secure Branch Operations

Challenge: Multiple branches with distributed CCTV, access control, and routers.
Solution: Centralized monitoring of NVRs/DVRs, firewalls, PoE switches, and CCTV feeds.
Benefit: Strengthens branch security and reduces downtime.

ObzoraNMS – Example Use Cases

Public Sector & Critical Infrastructure

Hospitals – Patient & Facility Safety

Challenge: Surveillance, access control, and medical IoT devices must remain operational.
Solution: Monitoring of switches powering IP cameras, UPS backup status, and device availability.
Benefit: Continuous operation of life-critical and security systems.

Smart Cities – City-wide Surveillance

Challenge: Thousands of street cameras, wireless backhauls, and NVRs need centralized monitoring.
Solution: GIS device mapping, wireless link health monitoring, automated camera downtime alerts.
Benefit: Proactive issue detection, improved public safety.

Government & Public Sector – Compliance & Transparency

Challenge: Regulations demand continuous video recording and high system availability.
Solution: Compliance-ready reporting, secure access roles, full monitoring of storage, UPS, and servers.
Benefit: Meets regulatory standards while maintaining transparency and uptime.

Hotels

Challenge: IP cameras, NVRs, and access systems across multiple floors require 24/7 uptime. Failures can create blind spots and compromise safety.
Solution: Real-time monitoring with alerts for device, storage, and power issues. Dashboards help teams quickly isolate problems.
Benefit: Ensures continuous surveillance, prevents recording loss, and maintains guest safety.

See Obzora NMS in Action

If you would like to **explore Obzora NMS further or see more features in action**, we invite you to book a live demo.

- **Scan the QR code** below to schedule your demo at your preferred date and time.
- Or visit **www.obzora.net** and go to the **Request a Demo** section.

Experience firsthand how Obzora NMS can simplify monitoring and ensure the uptime of your CCTV infrastructure.

SCAN ME

Connect US

Compliant Surveillance & Infrastructure Monitoring Platform

Address
23 Rue de la republique, 13002
Marseille, France

Call Us
+33 465 969 861

Email Us
info@obzora.net

UAE Distributor	
Meemtel IT Solutions Co. 208, Aim Business Tower, Al Qiyadah, Near to Metro station, Dubai-UAE	**Phone:** +971 50 284 5963 +971 50 373 0864 **Email:** info@meemtel.com