



VULTUREYE PSIM

Technical Datasheet

Unified Security & Intelligence Platform

Manufacturer: OMNIVISOR SAVUNMA SISTEMLERI YAZILIM DONANIM ELEKTRONIK A.S.

Email: info@omnivisor.tr

August 2026

Overview

Vultureye PSIM/VMS is a next-generation, enterprise-grade software platform designed for large-scale, multi-site security operations, unifying video management, physical security integration, and AI-powered analytics into a single federated platform. It brings together IP cameras, NVRs, access control, fire alarm, radar, acoustic sensors, X-ray screening, UAV/drone feeds, and many other subsystems into one command center. The software is developed within Turkey and is fully compliant with national and sovereign project requirements.

Technical Specifications

The tables below present the core technical specifications of the Vultureye PSIM/VMS platform, organized by category in a Feature–Value format.

1. General Architecture & Deployment

Feature	Description
Deployment Architecture	Client-server architecture; runs on Debian-based operating systems (Ubuntu, Pardus, etc.) without requiring an additional OS license.
High Availability (HA)	Supports 1+1 HA redundancy architecture for the VMS server, with automatic failover.
Federated / Multi-Site Architecture	Multi-site structure via VMS-to-VMS communication; a parent VMS can monitor devices under sub-VMS instances by IP, including historical recording playback and alarm viewing.
Horizontal Scalability	Streaming media server and recording service can each be scaled out horizontally without limit.
Flexible Deployment	Deployable on bare-metal, virtualized, or hybrid infrastructure; supports Linux and Windows Server environments, with web-based and native client interfaces.
Automatic Database Backup	Scheduled automatic daily database backup according to a defined interval.

2. Client Interfaces

Feature	Description
Client Applications	Desktop client, web client, and mobile client applications are available.
Operator Client Workstation	High-performance Windows operator client with flexible 1/4/9/16 split-screen layouts, instant live/playback switching, synchronized multi-camera playback (up to 4 cameras), and mouse/joystick digital zoom & PTZ control.

3. Camera, NVR & Video Integration

Feature	Description
NVR Integration	SDK-based integration with at least 4 NVR brands; supports playback and video export functions.
ONVIF Support	Supports ONVIF Profile S, G, T for cameras and Profile S, G, T, M for brand-independent IP camera integration.
IP Camera Integration	Brand-independent integration with at least 3 IP camera brands via API/SDK, in addition to ONVIF.

Feature	Description
Video Codec Playback	Plays H.264 and H.265 encoded video streams.
GPU-Accelerated Decoding	Performs video decode on CUDA-supported GPUs on client machines when available, with automatic fallback to software decoding under resource constraints.
IP Speaker Management	Manages IP speaker devices from at least 3 brands; ONVIF IP Speaker support enables two-way live audio and alarm-triggered audio file playback.
Virtual PTZ Control	Virtual PTZ panel supporting pan/tilt/zoom and preset call/set functions; compatible with all USB HID PTZ control keyboards.
ANR (Automatic Network Replenishment)	Synchronizes recordings between the camera SD card and the server; SD-card footage for a given date/time remains playable even without prior synchronization.
SD Card Playback Access	Provides brand-independent access to recordings stored on the camera SD card.
Alarm I/O Management	Manages camera alarm inputs/outputs and supports alarm box integration.
Remote Device Password Update	Passwords of ONVIF-compliant devices can be updated directly from the VMS interface.
Edge Analytics Integration	Edge analytics running on cameras (Dahua, Hikvision, i-PRO, Hanwha Vision, etc.) are integrated into the VMS via HTTP API/CGI/ISAPI.

4. Recording & Storage

Feature	Description
Server-Based Recording	Provides a dedicated external recording service (Omnistor Recording Service) in addition to NVR-based recording, supporting a fully server-based recording architecture.
Recording Codec Support	In the server-based recording architecture, records H.264/H.265 video streams received via ONVIF Profile S/T.
Recording Redundancy (N+1)	Recording service supports N+1 architecture; when the primary recorder goes offline the backup recorder takes over, and recordings are synchronized back once the primary returns online.
Recording Quota	Recording service can enforce a defined storage quota per camera.
Evidence Export	Supports full-resolution video export and high-quality JPG snapshot export, with an advanced archive-browsing interface and a tamper-detection mechanism for exported video.
Encrypted Video Export	Video exported through the recording service can be encrypted, so unauthorized parties cannot open it.
Live View Watermark	Overlays a watermark on live video to help deter unauthorized recording, e.g. via mobile phone.

5. Video Wall & Display

Feature	Description
Video Wall Management	Supports video wall management with decoder devices from at least 2 brands, plus local video wall and external controller support.

Feature	Description
Live View Layouts	Supports grid layouts such as 1, 2×2, 3×3, 4×4, 6×6; operators can save custom layouts as private or public and recall them at the next login.
Layout Sequencing	Automatically rotates through different layouts on selected screens at defined intervals.
Digital Zoom	Supports 1x, 2x, 4x, 8x digital zoom in both live view and playback.
Snapshot Capture	Snapshot capture is supported in both live view and playback.
2D Map / E-Map	Upload 2D map files (JPG, PNG) and pin cameras onto the map; clicking a camera on the map opens its live view.
GIS Integration	With internet access, cameras can be placed on a Geographic Information System (GIS) map for spatial situational awareness.

6. Network & Infrastructure Monitoring

Feature	Description
SNMP Network Monitoring	Reads network switch device status via IETF/IEEE-standard SNMP; tracks which device is connected to which port, including brand and model.
Redfish Server Monitoring	Monitors server hardware status — CPU model, fan status, RAID controller, PSU, etc. — via the Redfish standard, generating alarms per admin-defined rules on abnormal conditions.
Resource Health Monitor	Tracks CPU, GPU, and RAM consumption; monitors device online/offline status in real time; generates a full health report with one click.
Resource Threshold Alarms	Configurable CPU, RAM, and GPU thresholds trigger an alarm when exceeded.
Time Sync Alarm	Generates an alarm when the time difference between the system clock and a device clock (camera, NVR, etc.) exceeds a defined threshold.
Main Dashboard	Displays total device count, recently added devices, streaming media server status, database, and object storage status from a single screen.
Comprehensive Log Management	Comprehensive log management and health-monitor support; all user actions are recorded via the advanced logging infrastructure.

7. Alarm & Event Management

Feature	Description
Alarm Response Center	Runs scenario-based responses to edge-analytics alarms from integrated cameras of different brands: automatically opens the related live view, shows the alarm camera on the map, and retrieves the recorded clip and snapshot from the moment of the alarm.
Alarm Verification & Notes	Alarms can be marked true/false and annotated with operator notes as part of the alarm-response workflow.
Historical Alarm Records	Past alarms can be listed by time, type, device, and user, and reopened for review.
Generic Event Support	TCP/UDP-based generic event interface (port 13337) for receiving alarms from any third-party video analytics platform, simplifying integration; unlimited generic events can be defined.

Feature	Description
Acoustic Sensor Integration	Integrates with acoustic sensors that detect gunshots, screaming/aggression, glass breaking, drones, graffiti/spray, grinders, and car alarms/sirens, and displays the resulting alarms.

8. User, Role & Security

Feature	Description
User & Role Management	Users can be assigned to roles with defined permissions; permission management is also available for specific individual users outside their role.
Active Directory Integration	Domain users are synchronized with the VMS for centralized user management; scheduled automatic sync with OU-based or global (all-users) search support for large user bases.
Password Policies	Enforces password expiry for local users within a defined period, and supports active/inactive user status management.
Session Security	Automatically closes idle sessions after a defined period of inactivity, with a warning pop-up shown to the user beforehand.
IP Access Control	Supports IP blacklist/whitelist definitions to prevent unauthorized access, and suspends an IP address after a configured number of failed login attempts until manually unlocked.
HTTPS / TLS Security	Provides HTTP(S) connectivity with both self-signed and CA-signed certificate support, protecting against man-in-the-middle attacks.
Multi-Factor Authentication	CAPTCHA or 2FA options prevent large-scale brute-force login attempts; optional biometric facial-recognition login is also supported.
Audit Logging	Advanced logging infrastructure records all user actions, access events, and system events in detail for compliance and forensic purposes.

9. Licensing & Open API

Feature	Description
License Management	Supports offline licensing for environments without continuous internet connectivity.
OpenAPI Support	Management services and the recording service expose OpenAPI interfaces for third-party and custom integrations.

10. AI & Video Analytics

Feature	Description
AI Video Analytics	Brand-independent object detection on any camera brand using CUDA GPU-based AI servers, with free-text search for fast retrieval of relevant historical video moments.
OmniAI Integration	RESTful API-based integration with the OmniAI video-analytics management platform, which can operate standalone or fully integrated with Vultureye VMS.

Feature	Description
Face & License Plate Anonymization	AI-powered Face Anonymizer and Licence Plate Anonymizer modules for privacy-compliant footage sharing and review.
Prompt-Based Target Search	Free-text (prompt) based target search across recorded footage via the "VulturEye TargetSeeker" module.

11. Third-Party & Specialized Integrations

Feature	Description
Fire Alarm System Integration	Integrates with fire alarm systems from at least 3 brands, including Siemens, Tyco, Mavili, and Simplex.
Access Control Integration	Integrates with access control panels and readers from brands such as Dahua, OnPro, Hikvision, and HID.
Perimeter Radar Integration	Integrates with perimeter security radar systems such as Axis and Dahua, with SpotterRF planned for future integration.
X-Ray Baggage Scanner Integration	Via an encoder card, receives real-time X-ray baggage scanner video from any brand, stores it in the video storage, and supports analysis of objects passing through the scan tunnel.
Under-Vehicle Surveillance (UVSS) Integration	Integrates with a domestic under-vehicle surveillance system (MTM Bilişim), providing real-time under-vehicle and license-plate imagery and plate-based historical search.
UAV / Drone Integration	Receives live video from gyrocopters, DJI Enterprise-series UAVs, VTOL aircraft, and reconnaissance/surveillance balloons; authorized users can view feeds via the mobile app.
Fiber Optic Distributed Acoustic Sensing (FOTAS)	Integrates with a fiber-optic Distributed Acoustic Sensing (DAS) system (Samm Teknoloji) that detects acoustic waves and vibrations along long perimeter fences in real time.
IoT Platform Integration (MQTT)	An MQTT receiver and parser service ingests data from IoT/AIoT devices and edge-analytics alarms sent by modern cameras, with integration to the Thingsboard IoT platform.
SIEM Integration	Feeds Vultureye VMS and/or OmniAI events to SIEM platforms such as Logsign, IBM QRadar, Splunk, and ArcSight, using RFC 5424 / RFC 3164 syslog formats.
ARC (Alarm Receiving Centre) Integration	Provides alarm integration with the UK-based Immix ARC platform; OmniAI video-analytic alarm outputs can be fed into Immix.
Digital Twin Integration	Feeds video-analytic alarms to the Twinup digital-twin platform, delivering a 3D facility experience with enhanced situational awareness and ease of operation.
Operator Screen Monitoring (Evidence)	Monitors CCTV operator screens as evidence via a platform-independent agent (ITVDesk integration) or Vultureye's own native agent, to verify alarms were received and reviewed on time.
Body-Worn Camera Evidence Management	Supports integration of body-worn camera footage into an evidence-management platform.
Intrusion Alarm System	Integrates with SIA (Security Industry Association)-compliant intrusion alarm systems.

12. Localization & Reporting

Feature	Description
Multilingual Interface	Provides a multilingual user interface including Turkish and English, with customizable, role-based operator workspaces.
Domestic Development & Support	Developed and supported entirely within the borders of Turkey, with a local engineering and support team, ensuring compliance with national project requirements.
Reporting	System performance, device status, and user activity are available as compliance-ready reports, exportable in PDF, Excel, or CSV formats.

System Architecture & Topology

The diagrams below illustrate the overall deployment topology and integration ecosystem of the Vultureye VMS/PSIM platform.

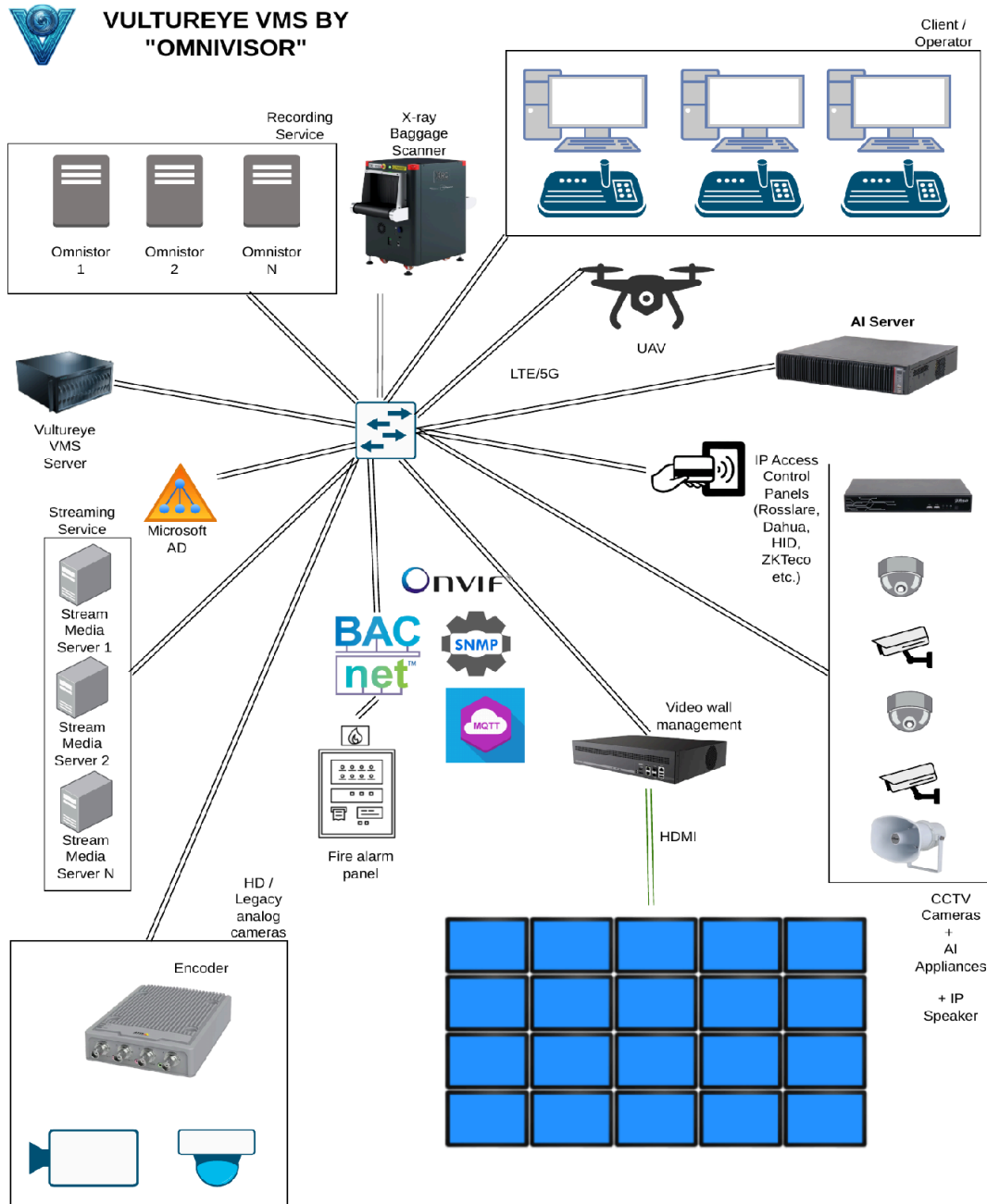


Figure 1 — Vultureye VMS Deployment Topology (by Omnivisor)

VULTUREYE VMS/PSIM INFRASTRUCTURE

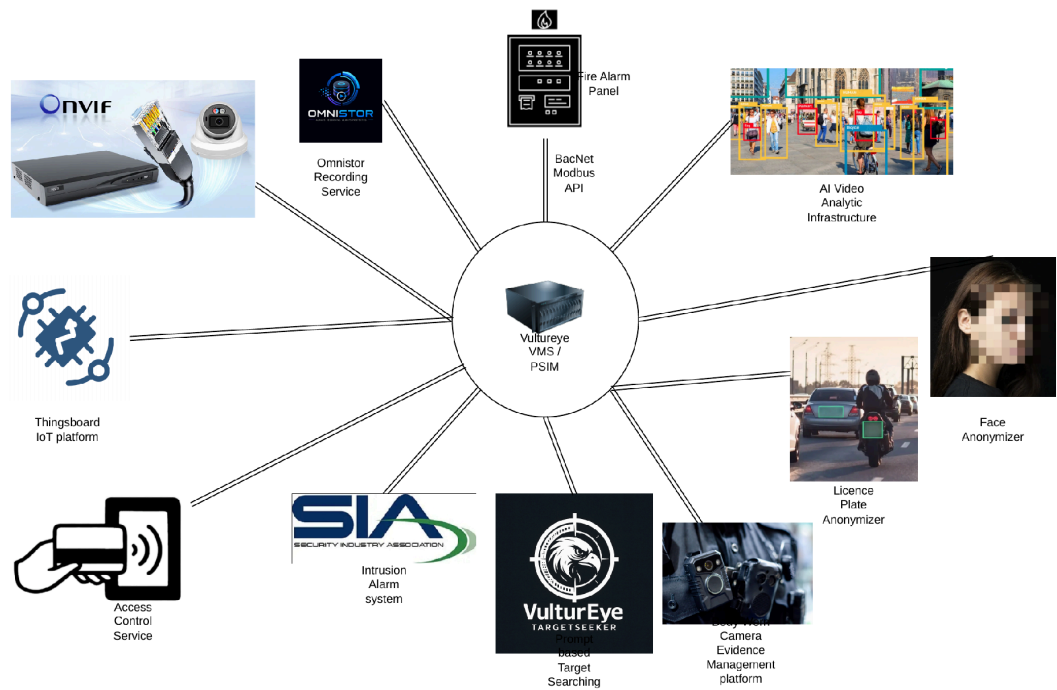


Figure 2 — Vultureye VMS/PSIM Integration Infrastructure

Integration Ecosystem & Supported Brands

Thanks to its open and extensible architecture, Vultureye integrates with a broad ecosystem of hardware and software partners.

Category	Brands / Partners
IPC / PTZ Cameras	Dahua, Axis, Tiandy, Hikvision, Hanwha Vision, Avigilon, i-PRO, Pelco — plus any ONVIF Profile S/G/T compliant brand
NVR	Tiandy, Dahua, Hikvision, i-PRO — plus Omnistor native recording service
Video Wall Decoders	Hikvision UDI69xx series, Dahua NVD series (NVD0405/1205/1605), NVIDIA CUDA GPUs, Barco, 4thewall
Perimeter Security Radar	Axis, Dahua (SpotterRF planned)
IP Speakers	Dahua, Axis, Commend, Hikvision
Network Switches (SNMP)	Juniper Networks, Cisco, Planet, Extreme Networks
Server Monitoring (Redfish / IPMI)	Dell iDRAC, HP iLO, Supermicro, Huawei iBMC
Fire Alarm Systems	Siemens, Tyco, Mavili, Simplex
Access Control	Dahua, OnPro, Hikvision, HID
X-Ray Baggage Scanners	XRC, Astrophysics, Hikrayin, Dahua, Rapiscan, and more
Under-Vehicle Surveillance (UVSS)	MTM Bilişim
Acoustic Sensors	Jalud Embedded
Fiber Optic Acoustic Sensing (FOTAS)	Samm Teknoloji
IoT / MQTT & IoT Platform	Milesight, Terjin, Thingsboard
SIEM	Logsign, IBM QRadar, Splunk, ArcSight
ARC (Alarm Receiving Centre)	Immix (UK)
Digital Twin	Twinup
Operator Screen Evidence	ITVDesk, Vultureye native agent
UAV / Drone Platforms	Gyrocopter, DJI Enterprise series, VTOL platforms

Recommended Server Hardware

The recommended minimum hardware configuration for a standard Vultureye VMS/PSIM server deployment is provided below.

Component	Recommendation
CPU	2× Xeon/EPYC, or 1× high-core-count processor — 16–24 cores
RAM	64 GB
System Disk	2× 960 GB–1.92 TB NVMe, RAID 1
MinIO / Object Storage	2–4 TB NVMe (alarm JPEG/WAV metadata; not full video)
Network Interface (NIC)	2× 1 GbE
Operating System	Ubuntu 22.04 / 24.04 LTS

Recommended Client Hardware

The recommended hardware configuration for operator workstations is provided below.

Component	Recommendation
CPU	Intel Core i7-14700
RAM	32 / 64 GB
GPU	NVIDIA RTX 4500 Ada or RTX A5000
Storage	1 TB NVMe
Network	1 / 2.5 Gbps
Display	1× 4K monitor

This document is for informational purposes; technical specifications are subject to change without prior notice.