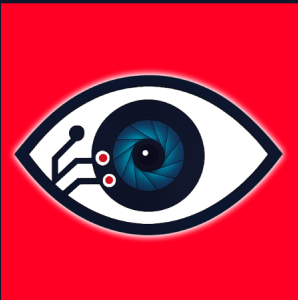


We turn existing security cameras into an early-warning system

CamGuard AI analyzes the feed from the ONVIF/RTSP cameras a business already runs; it detects flame, smoke, people, and vehicles, and sends an alert over five channels within seconds.



PRODUCT OVERVIEW

www.camguard.ai · support@camguard.ai · +90 555 595 26 00

July 2026

THE PROBLEM

The cameras are there, but nobody is watching

Hundreds of thousands of businesses already have camera infrastructure in place. Yet almost every one of those systems is a **recording device, not an alerting device**. The footage is looked at only after something has happened.

Fire is noticed too late

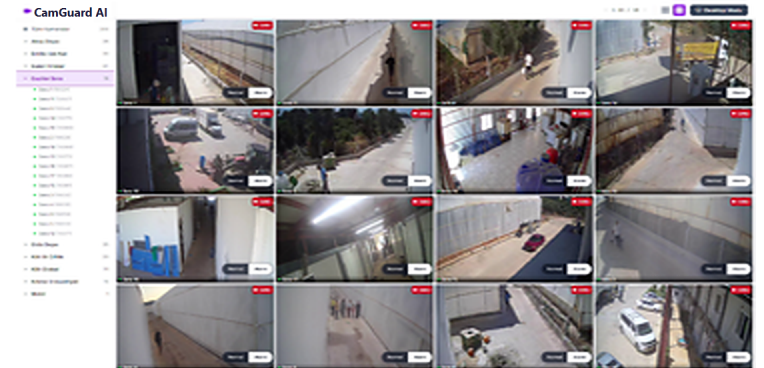
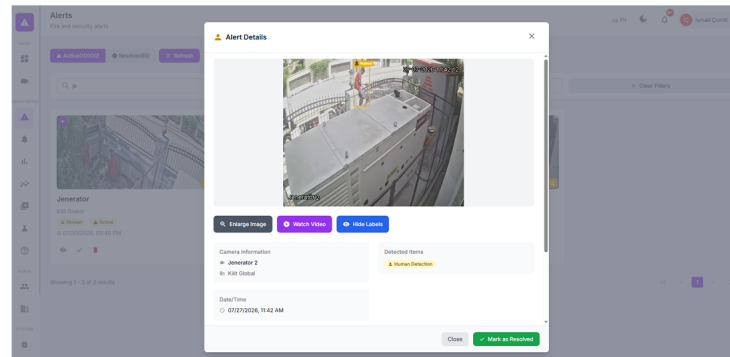
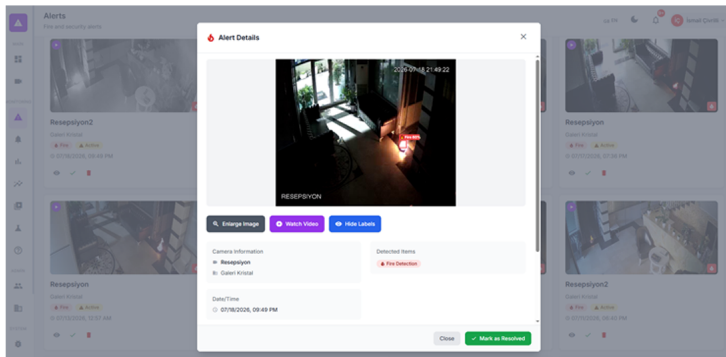
A smoke detector waits for smoke to rise to the sensor. In a high-bay warehouse, a greenhouse, or an open yard it is far too late, or never. The first 5 minutes decide a warehouse fire.

Theft is seen afterwards

A motion sensor cannot tell a swaying branch, a passing animal, and a shadow apart. A system that keeps crying wolf gets switched off — and nobody is warned when it matters.

Nobody watches screens 24/7

On a site with dozens of cameras it is simply not possible for a guard to follow every screen without a break. On the night shift the odds drop further.



The result: camera infrastructure that has already been paid for is used to produce evidence after the event instead of preventing it. The missing piece — a layer that reads the picture in real time — has stayed unfilled because it used to be expensive and complex.

How does CamGuard AI work?

No new cameras, no new cabling, no thermal hardware. The feed from the existing cameras goes to a GPU field server installed on site; the analysis happens there.

1

Integration

Existing ONVIF/RTSP cameras are registered on the field server. Brand-independent; analog cameras connect through the NVR.

2

AI analysis

The GPU server on site analyzes every camera 24/7 without a break. Live video never leaves the premises.

3

Detection and verification

Flame, smoke, or unauthorized entry is detected; multi-layer filters and a second-stage visual check remove false alarms.

4

Instant alert

Five channels fire at the same time; the event video and evidence frame are archived.

Existing cameras

No new hardware investment

No thermal needed

Standard IR night vision is enough

Does not replace the NVR

Adds an analysis layer on top

Live in one business day

If the cameras are ready

Four detection types, one platform

Flame detection

Flame is picked up the moment its glow enters the camera's field of view. It works in night vision too: the system recognizes from the picture itself that the camera has switched to black-and-white, and applies night-specific criteria.

Smoke detection

The model is trained to recognize both flame and smoke. In smoldering fires smoke becomes visible before flame does, which makes it critical for early warning.

People / unauthorized entry

It looks for a **person**, not motion. Branches, animals, rain, and shadows raise no alarm. Each camera defines which zone is watched at which hours.

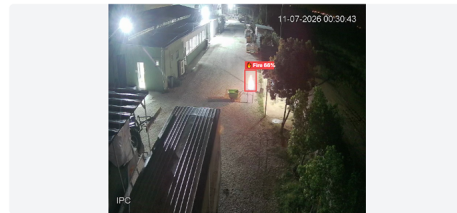
Vehicle detection

Can be defined as a separate rule. Parked, stationary vehicles are filtered out; at night the glare of headlights is told apart from flame.

Zone and time rules are defined separately for every camera. Example: a welding bay is left out of monitoring during shift hours and automatically returns to fire and person monitoring once the shift ends.



Enlarge Image Watch Video Hide Labels



Enlarge Image Watch Video Hide Labels



Enlarge Image Watch Video Hide Labels



Enlarge Image Hide Labels

A detection does not become an alarm

Most projects in this field fail not for technical reasons but **because of false alarms**. A system that keeps going off for nothing is first ignored, then switched off. In CamGuard AI every detection passes through filters in sequence.

1

Physical filters

Size, aspect ratio, texture variance.
Flat, smooth glare (lamp glass, headlight) is dropped.

2

Static light filter

Glare that keeps appearing at the same spot is learned and taken off the alarm list.

3

Persistence and growth

Real flame flickers and grows. A single-frame flash raises no alarm.

4

Day / night mode

Streetlights and headlights are not mistaken for flame; night-specific thresholds apply.

5

Visual verification

An event that clears the filters is confirmed against the same scene in its normal state.

6

Zone and time rules

Known sources (welding bay, stove, exhaust) are excluded at defined hours.

7

Vehicle / headlight split

Glare overlapping a vehicle and glare from headlights are judged separately.

8

Static object filter

A mannequin, a poster, or a hi-vis jacket on a hook does not alarm again and again.

Why it decides everything: whether a security system survives in the field is settled by this layer.

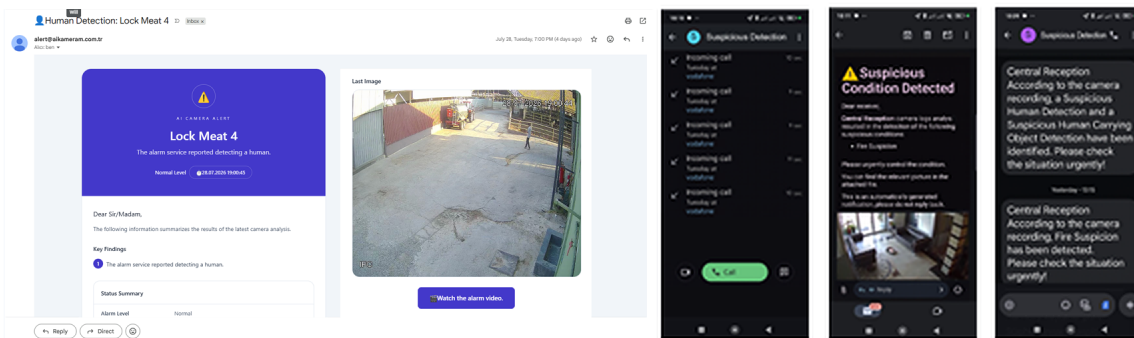
Five channels, at the same time

- **Automated phone call** — the system calls your contacts automatically and states the type and location of the event.
- **SMS** — a short alert with the camera name and the time.
- **Email** — a snapshot of the moment, with camera name, location, and time.
- **Mobile push notification** — instantly, to panel users.
- **On-site alarm device** — a loud siren, a flashing red fire/intruder icon, and the type and location of the event on an LCD screen.

Which camera notifies whom, and at which hours, is set from the panel. Channel and alarm type are chosen per user; the event video and evidence frame are archived.



On-site alarm device — siren, illuminated fire/intruder icon, and LCD screen. It keeps working even when the internet is down, powered from the field server.



Analysis on site, management at the center

The live camera stream **never leaves** the premises. Only the evidence frame and the event record of a verified alarm reach the central panel. That is decisive for privacy and for bandwidth alike.

Field (edge) server

Inside the facility, on the same network as the cameras. 24/7 analysis on GPU. Hardware scales with camera count, from a single-board edge device to a multi-GPU server.

Central panel

Every site is monitored from one panel. Organization- and user-level permissions, event archive, video recording, reporting, and notification settings.

Data privacy compliance

Personal data is processed where it arises. Access logs, retention controls, and user-level permissions in the panel. Guidance on notice and signage duties is provided at setup.

~105 kbps / camera

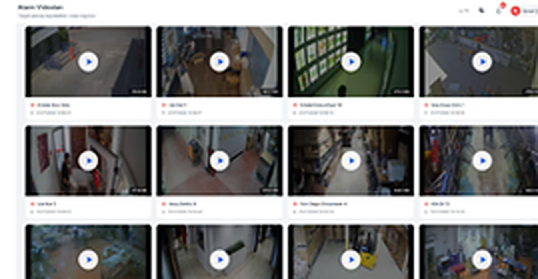
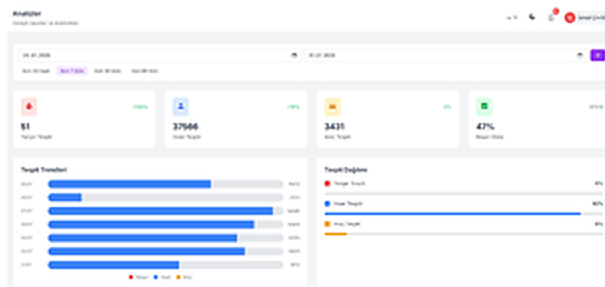
Average traffic from the field server to the center. There is no continuous video upload.

Works through outages

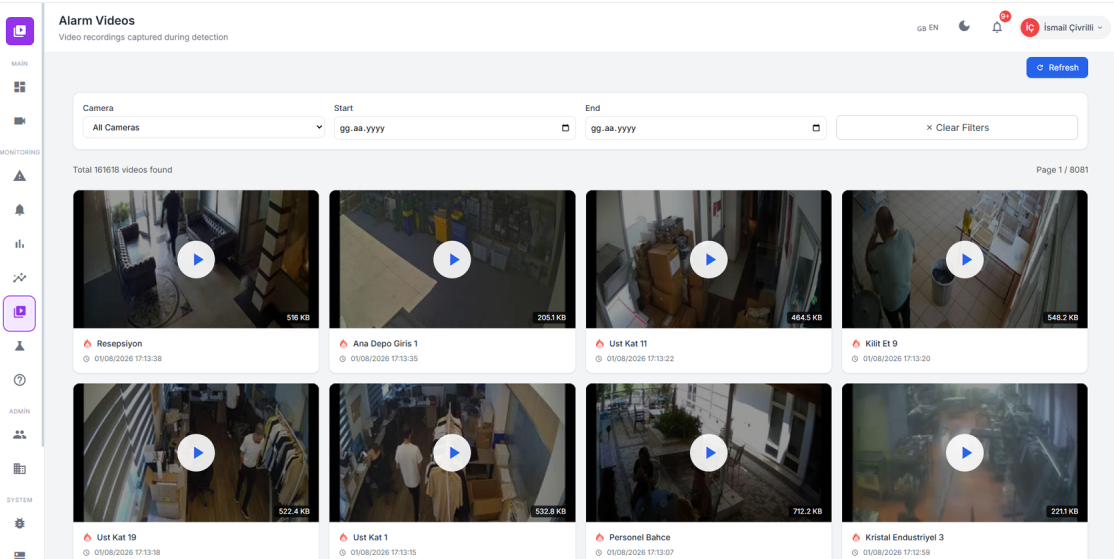
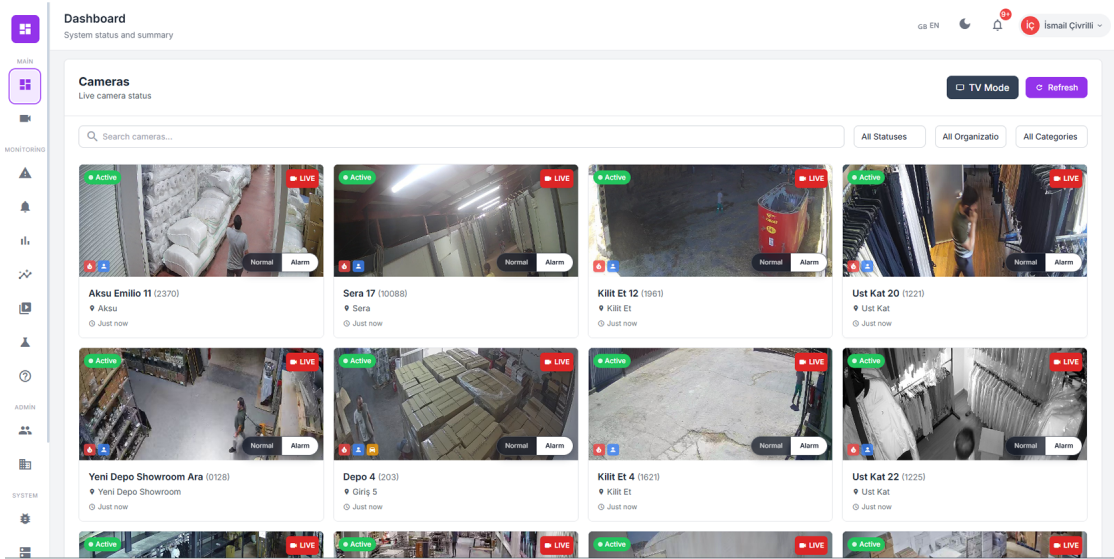
Analysis and the local alarm device carry on; queued alerts go out when the link returns.

Your NVR stays

The recording system stays in place; CamGuard AI reads and analyzes the same stream.



Every site on one screen



Live event tracking
Real-time notice in the panel as an alarm fires

Event and video archive
Evidence frame + event video

Zone and time rules
Drawn directly on the camera image

Multi-organization access
Permissions per organization and user

Twelve industries with a defined deployment scenario

All of them sit in the SMB and enterprise segment that operators already serve with fiber and mobile.

Factory and manufacturing Electrical panel and machine fires, welding sparks	Distribution warehouse Fire spreading fast on high racking	Recycling / waste The highest fire risk of any industry	Greenhouse and agriculture Heating unit, plastic sheeting catching fire
Livestock farm Straw and feed storage fires	Gas station Fast-growing fuel fires	Construction site Cable, copper, fuel, and equipment theft	Lumber / wood Sawdust and dust igniting fast
Textile Fabric piles, cotton dust, machines overheating	Energy and substations Noticed late on unmanned sites	Parking lot Fires in the EV charging area	Apartments, mall, hotel Mechanical room fires, perimeter line

Not a pilot — a system running in the field

CamGuard AI is in uninterrupted production today across different industries and different network and hardware conditions. The figures below are the current state of the live system.

680

cameras under 24/7 AI analysis

24

field servers

10

organizations run from one central panel

<55,000

recorded events (with evidence frame and video)

Industry diversity

Food and distribution warehouses, industrial plants, greenhouses, livestock farms, showrooms, and hotels — each with its own false-alarm sources and its own working hours.

Hardware flexibility

The same software, from a single-camera portable setup to a **100**-camera multi-GPU server. x86 servers and ARM-based edge devices (NVIDIA Jetson) are supported; on a small site the cost drops.

WHAT IS DIFFERENT?

Compared with existing solutions

CamGuard AI does not replace a smoke detector or a recording system; it adds a **visual early-warning layer** exactly where neither of them can see.

TOPIC	SMOKE DETECTOR / MOTION SENSOR	CAMGUARD AI
Trigger condition	Smoke physically reaching the sensor; or any movement at all	Flame, smoke, a person, or a vehicle being seen by the camera
Open areas and high ceilings	In practice does not work, or is far too slow	Protects wherever the camera looks; no delay
False alarms	Branches, animals, shadows, dust, and steam set it off	Eight filter layers + visual verification; it looks for an object , not motion
Location detail	By zone	Which camera, and where in the frame — the exact spot
Evidence	None	Snapshot and video of the moment, archived
Installation	Wiring and sensor mounting	Uses the existing cameras; one business day if they are ready
Rule definition	Fixed; limited control over hours and zones	Zones drawn on the camera image + time rules, per detection type

SUMMARY

CamGuard AI in brief

Builds on the existing investment

No new cameras, no new cabling, no thermal hardware. The installed ONVIF/RTSP infrastructure is used brand-independently; the NVR stays put.

Warns before the event

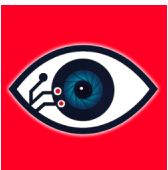
Flame, smoke, people, and vehicles are detected the moment the camera sees them; an alert goes out over five channels within seconds.

Does not produce false alarms

Eight filter layers and a second-stage visual verification. Zone and time rules exclude the known sources.

Video never leaves the site

Analysis runs on the field server; only the alarm evidence goes to the center. Privacy-first design, ~105 kbps per camera.



CamGuard AI — for a demo and more detail

www.camguard.ai · support@camguard.ai · +90 555 595 26 00 (phone and WhatsApp)