



WHITE PAPER

From Alert to Action: Putting AI Video Analytics into Operation

A practical method for AI video analytics: choosing use cases, red-team piloting, routing alerts into existing alarm workflows, tuning, privacy and scale.

By IoT Hybrid Solutions

AI VIDEO ANALYTICS

GSOC

PILOTS

ALARM MANAGEMENT

PRIVACY



Executive summary

- AI video analytics creates value only when an alert leads to a faster, better decision by an operator. Start from the operational problem, not the feature list.
- Pilot in phases with written success criteria, and test across every shift with blind red-team scenarios run by your own security operations team.

- Deliver alerts into the alarm workflow operators already use. A new pane of glass adds work instead of removing it.
- Expect tuning. Plan for it, measure false alarms honestly and re-test after every change.
- Prefer behavior-based detection over identity-based processing where it meets the need, and involve privacy and legal teams before activation.

Selecting use cases

The strongest use cases share three traits: the event matters, operators currently miss it or spend too long on it, and a defined response exists.

Common categories

- **Access-related:** door forced, door held or propped, unauthorized entry, tailgating at turnstiles or doors, a person loitering near an exterior door
- **Intrusion:** presence in a restricted area after hours, crowd formation, perimeter approach
- **Safety:** person down, smoke or fire, unattended bag, sudden egress, fighting, visible weapon
- **Situational:** unattended reception desk, animals on site, emergency personnel arrival
- **Investigative:** search by appearance, attribute or natural-language description across recorded video

Prioritizing

Score candidate use cases on:

- Risk reduction if the event is detected sooner
- Current operator effort, such as nuisance door alarms that each require video review
- Availability of suitable camera views and lighting
- Clarity of the response procedure
- Privacy sensitivity

A useful early target is often nuisance alarm reduction: analytics that review a door forced or held alarm and clear it automatically when video shows no person, so operators see fewer alarms that need no action.

Piloting method

A pilot should answer a decision question: is this worth deploying more widely, and on what terms?

Phases

1. **Prepare:** select cameras and doors, confirm network and compute requirements, commission the system, hold a kickoff, and train operators.
2. **Enable:** turn on detections in a monitored state, confirm alerts arrive correctly, and fix integration issues.
3. **Operate:** run the analytics alongside normal procedures for several weeks, logging every alert and its disposition.
4. **Evaluate:** compare results with success criteria, hold a business review and decide: scale, extend the pilot or stop.

Success criteria

Write criteria before the pilot starts. Typical measures include detection of defined scenarios, false alerts per camera per day, time from event to operator alert, operator workflow fit, investigation time savings and integration reliability. Agree the targets with operations leadership so the evaluation is not a matter of opinion.

Red-team testing across shifts

Live operations alone may not produce enough real events to judge detection. Supplement them with structured tests:

- Run scenarios during day, swing and night shifts to capture lighting, staffing and traffic differences.
- Make some tests blind to operators so you measure the real workflow, not a prepared one.
- Have your GSOC or security team design and run the scenarios, with safety controls and site notifications in place.
- Record each test: time, location, expected detection, actual result, operator response.
- Re-test after any tuning or vendor fix.

Pilot infrastructure

Pilots often use temporary compute, such as an edge appliance, and a limited set of camera streams. Confirm who provides network ports, VLANs and firewall changes (typically the customer's IT team) and whether any power or cabling work is needed (typically the customer's trades unless

contracted to the integrator). At the end of the pilot, decommission temporary equipment and obtain written confirmation that pilot data has been deleted.

Integrating alerts into existing workflows

Operators already have an alarm console, procedures and a dispatch path. Analytics should feed that workflow, not compete with it.

Integration principles

- **One alarm queue:** write analytics alerts into the existing video management or alarm monitoring platform as alarm events, ideally one event type per detection so each can carry its own priority and procedure.
- **Two-way context:** bring access control events (forced, held, invalid badge, granted and denied) into the analytics engine, and send analytics results back to the platform.
- **Linked video:** every alert should open the relevant live and recorded video with one action.
- **Procedures attached:** each alert type should map to a documented response, such as verify, dispatch, notify or close.
- **Escalation path:** confirm how alerts reach dispatch, mass notification or first responders where appropriate.

Operator readiness

- Train operators on each alert type with real examples from the pilot
- Provide a playbook and short reference sheets at each console
- Review alert dispositions with shift supervisors weekly during the pilot
- Capture operator feedback on noise, priority and usability

Tuning and false-alarm management

No analytics system performs perfectly on day one. Plan and budget for tuning.

What to tune

- Detection zones, masks and minimum object sizes
- Schedules, so detections run only when they are meaningful
- Sensitivity and dwell thresholds

- Camera position, field of view, focus and lighting, which often matter more than software settings

Managing false alarms

- Define what counts as a false alert, a nuisance alert (correct detection, no action needed) and a missed detection
- Track each category by camera and by detection type
- Prioritize tuning for the cameras that generate the most noise
- Escalate persistent issues to the vendor with evidence, and re-test after fixes
- Report honestly: a detection that needed tuning is a normal finding, not a failure

Privacy by design

Video analytics can raise privacy concerns among employees, visitors and regulators. Address them before activation, not after.

Behavior-based versus identity-based

- **Behavior-based analytics** detect events and objects, such as a person in a restricted area or a door held open, without identifying who the person is.
- **Identity-based analytics** such as facial recognition process biometric data and are subject to additional legal requirements in many jurisdictions.

Where behavior-based detection meets the operational need, it generally carries lower privacy risk. Appearance search by clothing or attributes sits between the two and deserves its own review.

Privacy checklist

- Document the purpose of each use case and the data it processes
- Complete a privacy or data protection impact assessment where required
- Confirm retention for alerts, clips and metadata, and align with existing video retention policy
- Restrict access to analytics search by role, and log its use
- Update signage and notices where required
- Consult employee representatives and counsel on applicable laws in each jurisdiction

Measuring value

Measure outcomes that leadership recognizes, and baseline them before the pilot.

- Reduction in nuisance alarms requiring operator review
- Time from event to operator awareness, and from awareness to response
- Investigation time for common incident types
- Events detected that would previously have been missed
- Operator workload and console time per shift
- Alternatives avoided, such as additional turnstiles or guard posts where tailgating detection meets the need

Avoid converting these into savings figures without agreed inputs from finance and operations. A separate business value assessment, using your own staffing and cost data, is the right place for that.

Scaling decisions

A successful pilot answers whether to scale. The next question is how.

Decision criteria

- Did the detections that matter meet the success criteria, including after tuning?
- Did alerts fit the operator workflow without adding work?
- Is the integration stable enough for production?
- Are privacy approvals in place for the wider footprint?
- Is there a clear priority order for expansion, such as the doors with the highest alarm volume?

Planning the rollout

- Size compute, storage and network for production, not pilot, volumes
- Confirm licensing model and lifecycle costs
- Define who maintains tuning and models after rollout
- Set ongoing reporting so value is measured continuously
- Schedule periodic red-team tests to confirm performance over time

How IoT Hybrid Solutions can help

IoT Hybrid Solutions designs and runs vendor-neutral analytics **pilots**, integrates alerts into your existing video and alarm platforms, and supports production rollout through **integration** and **managed services**. We work with analytics providers such as Ambient.ai and BriefCam as examples, alongside your existing platform, and we state up front which network, power and cabling work belongs to your IT and facilities teams. See also **video solutions** and **command and control**.

Next step

If you are considering AI video analytics, a structured pilot is the fastest route to a defensible decision. **Contact us** to scope one.