Operational Intelligence for Regulated Environments

Upgrading passive CCTV into GMP-aware security, safety, and compliance networks.

The Blind Spot

Security and QA teams cannot continuously monitor every entry, gowning area, corridor, lab bench, and storage room.

The Consequence

Compliance Risk

GMP and SOP deviations lack fast visibility and timestamped evidence.

Safety Risk

Unauthorized access to cleanrooms, restricted labs, and documentation areas goes unnoticed until post-incident.

Operational Drag

Manual video review after incidents, audits, or deviations is slow, reactive, and difficult to correlate.

Passive Recording vs. GMP-Aware Intelligence

	Current State (Passive CCTV)	Future State (Camsense AI)
Monitoring Method	Manual human review	**Tireless, automated observation**
Incident Response	Post-event forensics	**Real-time role-based alerts**
SOP Compliance	Blind spots & assumptions	**Visible, verifiable process discipline**
Audit Evidence	Hours of raw, unsearchable footage	**Searchable timestamped logs & clips**
Infrastructure Need	Full system rip-and-replace	**No-code intelligence overlaid on existing cameras** (CCTV/IP/NVR/RTSP)

Trigger-to-Insight

The Input

Connect compatible existing feeds without hardware replacement.

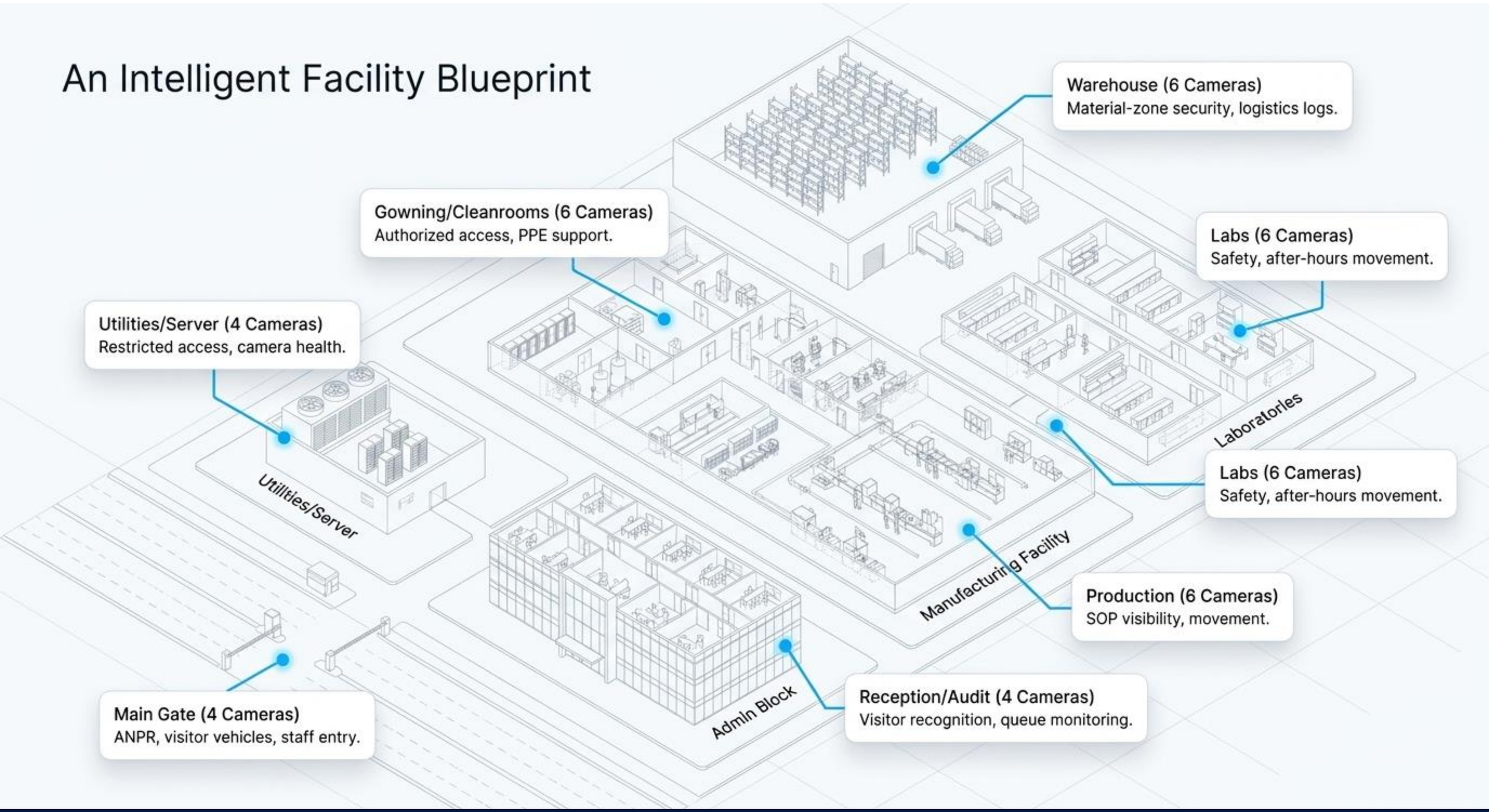
The Engine
Camsense Edge AI Box

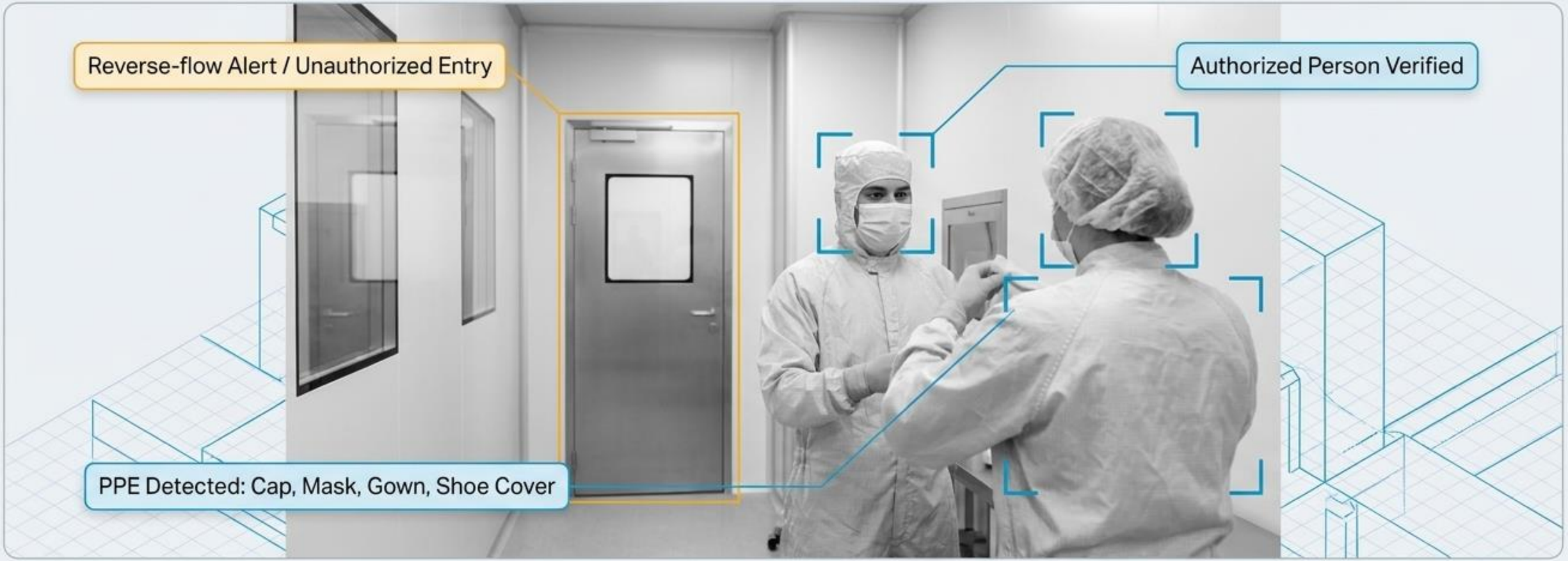
Configure restricted-zone, safety, and operations rules without code.

The Output

Real-time detection of movement, hygiene, and compliance exceptions turns into searchable evidence history and dashboard reports.

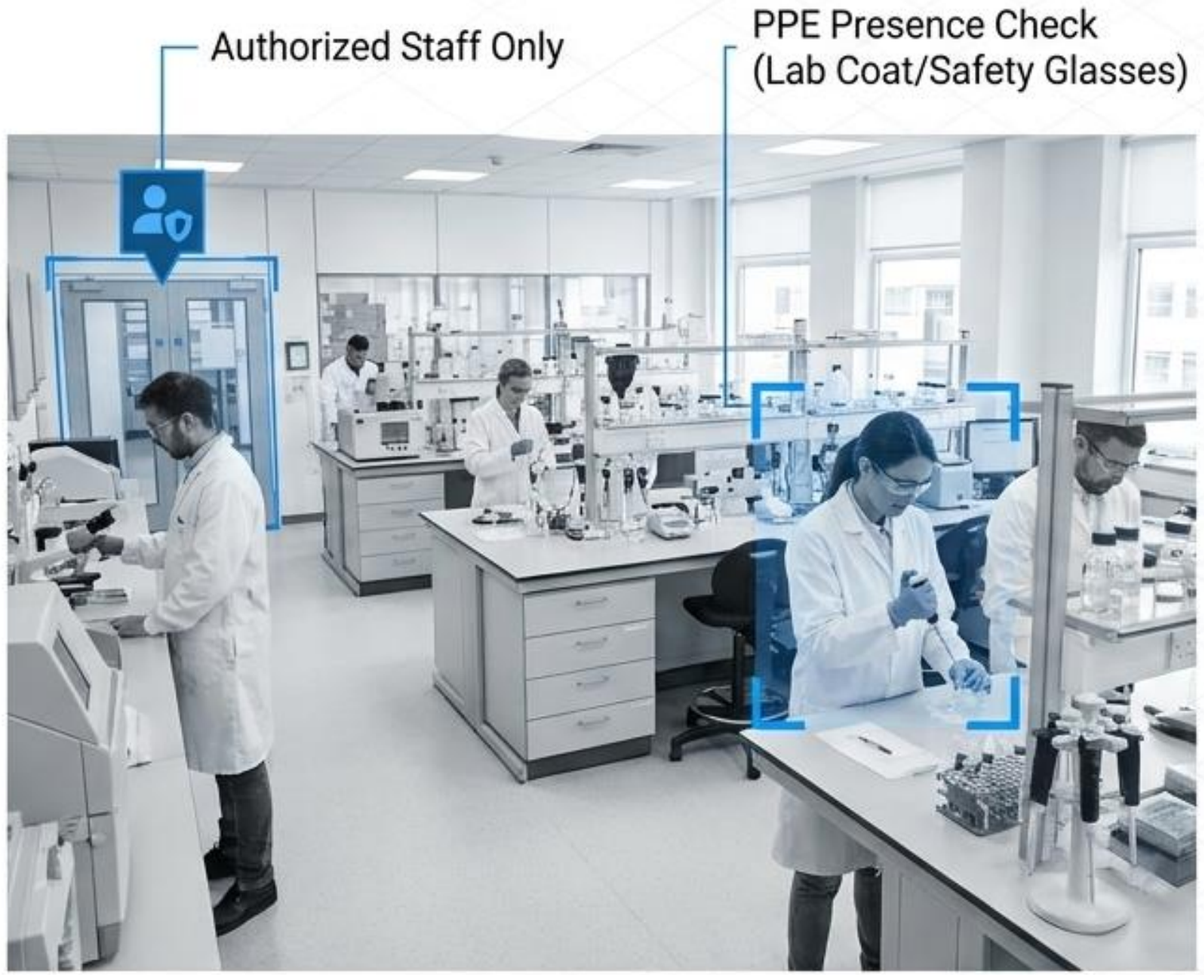
An Intelligent Facility Blueprint



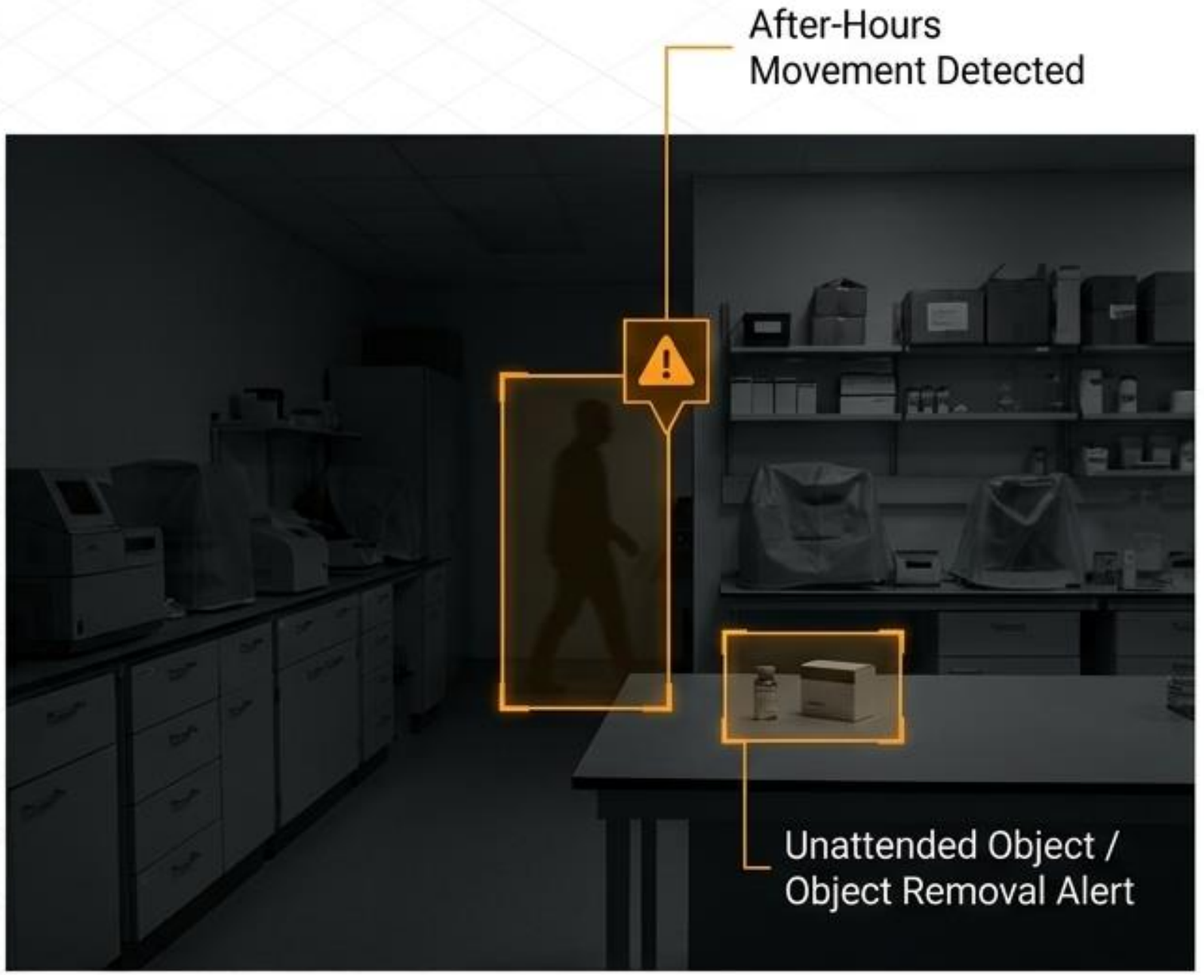


Supporting Disciplined Cleanroom Entry

Camsense monitors visible process discipline, queue crowds, and gowning sequences in **real-time**. It acts as an **operational intelligence layer** for visible compliance, while recognizing that absolute microbial and particle compliance remains strictly within the purview of validated QA environmental systems.



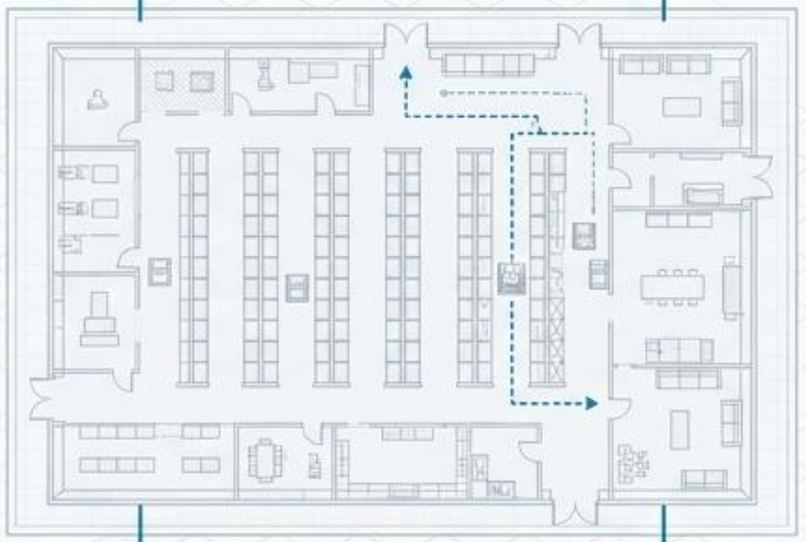
Safety & Access Monitoring

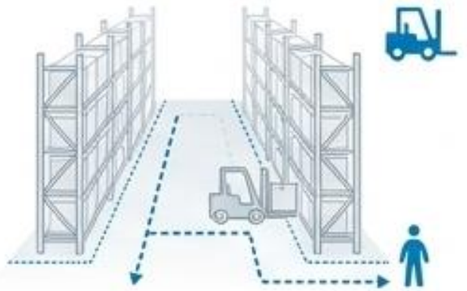


Asset & Sample Protection

Evidence clips are automatically generated for sample-handling disputes, safety events, and incident investigations.

Restricted Zones:
Securing quarantine and controlled substance areas.





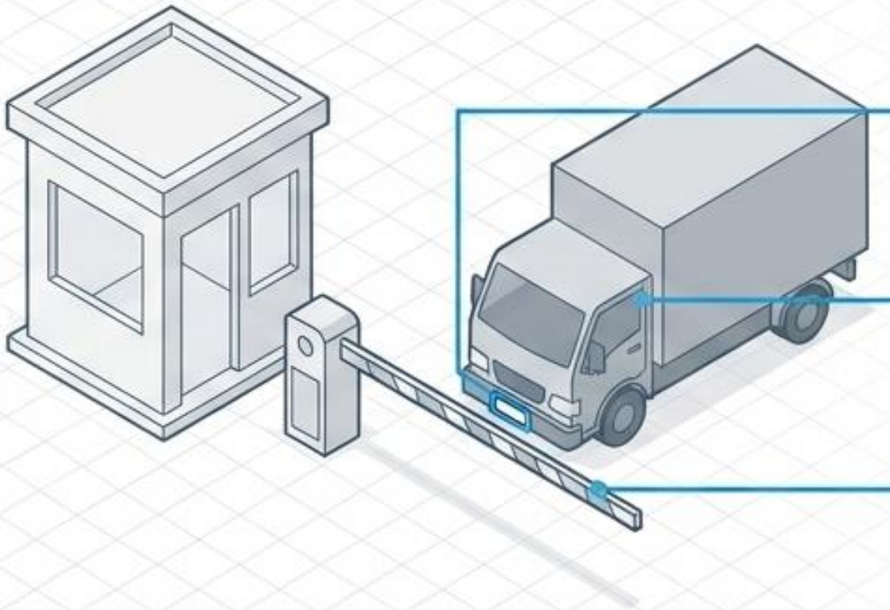
Logistics Flow:
Vehicle/pedestrian zone monitoring and wrong-parking alerts.

Crowd Control:
Line-entry shift changes and Queue Density Alert metrics.

Safety Continuity:
Visual fire/smoke detection and camera health loss alerts.

Designed to support safety and traceability—working alongside, not replacing, MES, ERP, or validated batch records.

ANPR Intelligence



- Automatic logging of plate numbers
- Categorizing employee vs. vendor vehicles
- Measuring gate congestion & peak-hour logistics

Facial Recognition & Watchlists

- Authorized staff entry logs for approved gates.
- Identity verification for QA/QC heads and supervisors.
- ⚠ Watchlist alerts for banned visitors or terminated staff.

Active EHS & SOP Escalation Workflows

Event
(Camera)

Camera detects a blocked emergency exit or tailgating at a badge door.

Processing
(Edge AI)

Local server classifies the severity and event type in real-time.

Escalation
(System)

Automated routing to the correct team (e.g., EHS for blocked exit, QA for PPE).

Resolution
(Human)

Team reviews evidence clip, takes action, and documents CAPA in approved systems.

The Command Dashboard: From Raw Video to Traceable Evidence

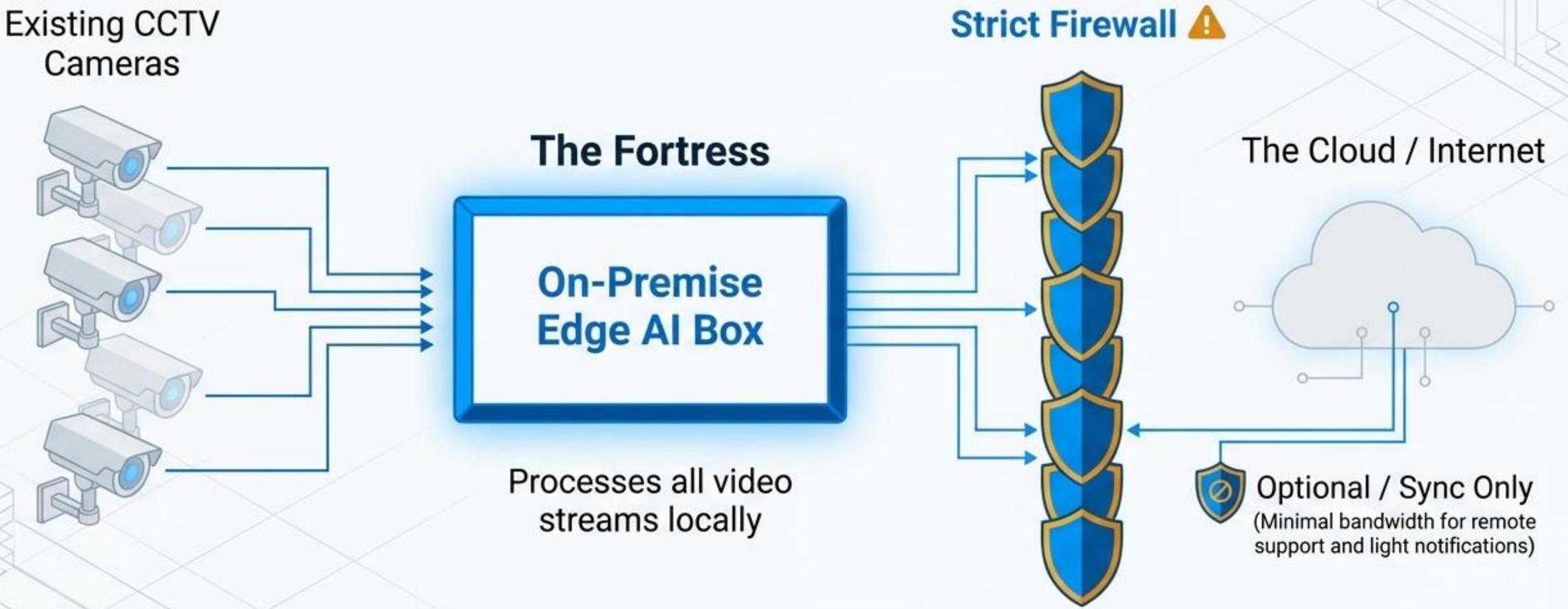
1 Real-time Alert Feed
Shows event type, camera, zone, timestamp, and severity.

3 Search Matrix
Filter history by person, vehicle, zone, or event type.

2 Evidence Viewer
A highlighted snapshot/clip attached to an alert for instant verification.

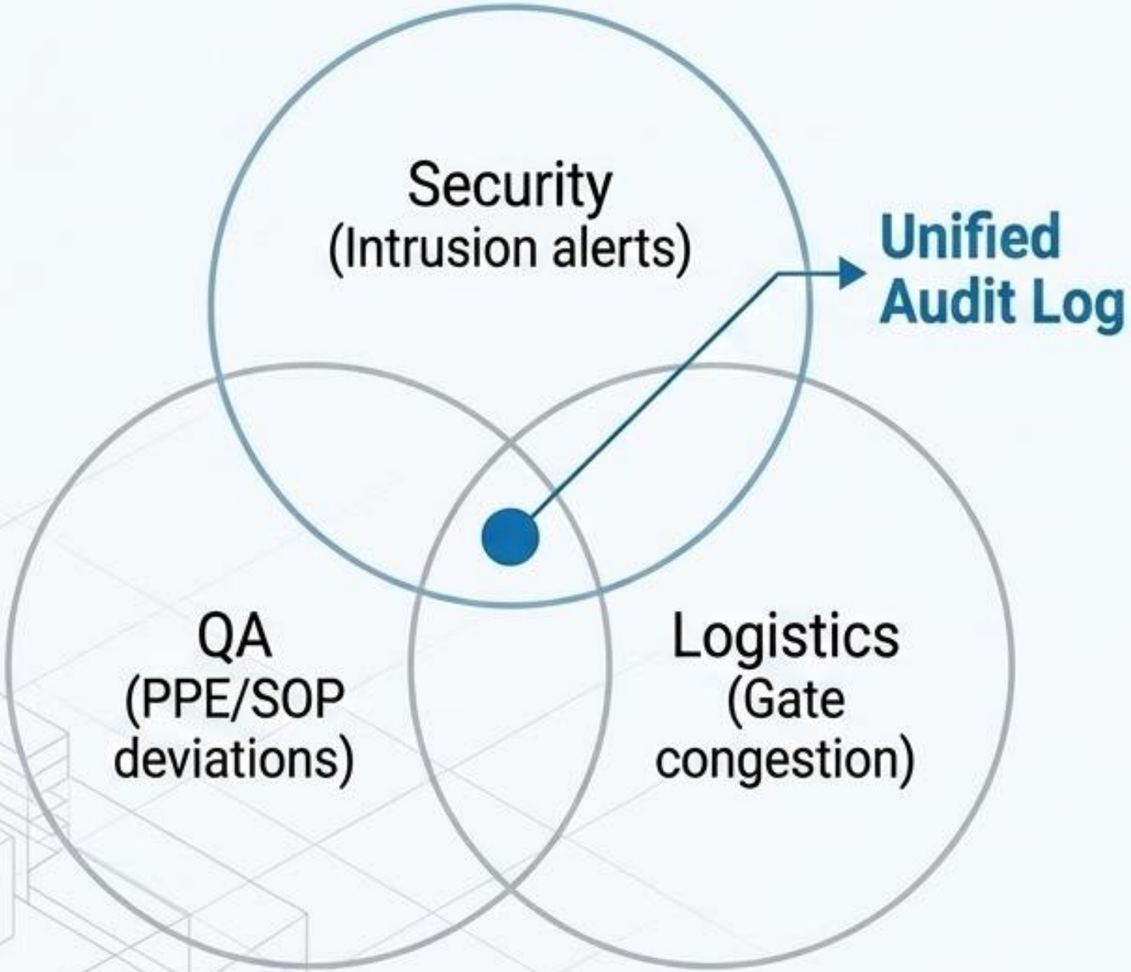
4 Reporting Engine
Automated daily/weekly reports routed to specific facility and management teams.

Edge-First Deployment Architecture



Sensitive video data never unnecessarily leaves the facility walls. **Hardware sizing scales logically with camera count, resolution, and concurrent analytics.**

Role-Based Access Control



Strict Governance Checklist

Consent & Privacy

Facial recognition requires explicit enrollment, HR/QA approval, and transparent notices. Private spaces such as washrooms and changing rooms are strictly avoided by design.

Decision Support, Not Replacement

AI alerts serve purely as timestamped evidence. Definitive GMP conclusions and formal CAPA decisions remain strictly governed by approved human QA processes.

An Ownership-Friendly Commercial Model

Existing Cameras
(Sunk cost / Retained value)

+

One-Time Software License
(Based only on scoped cameras and approved use cases)

+

Annual AMC
(Kicks in from Year 2 for support)

+

Edge Hardware (Optional)
(GPU, storage, networking at actuals)

=

A transparent capital expenditure model without heavy default SaaS lock-ins, tailored after a site survey and IT/Security technical validation.

The 30–45 Day Validation Pilot

Week 1: Survey & Scope

Camera audit, QA/Privacy review. Select 3–5 use cases across 10–20 priority cameras (e.g., cleanroom entry, main gate).

Week 2: Infrastructure

Edge/server prep, secure network approval, and initial camera onboarding.

Weeks 3–4: AI Tuning

Rule setup, facial enrollment workflow, live alert tuning, and ANPR/PPE testing.

Weeks 5–6: Handover

Delivery of first QA/Security management reports, evidence workflow review, and scale blueprint design.

Start with the zones where missed events affect compliance, safety, or operations the most.