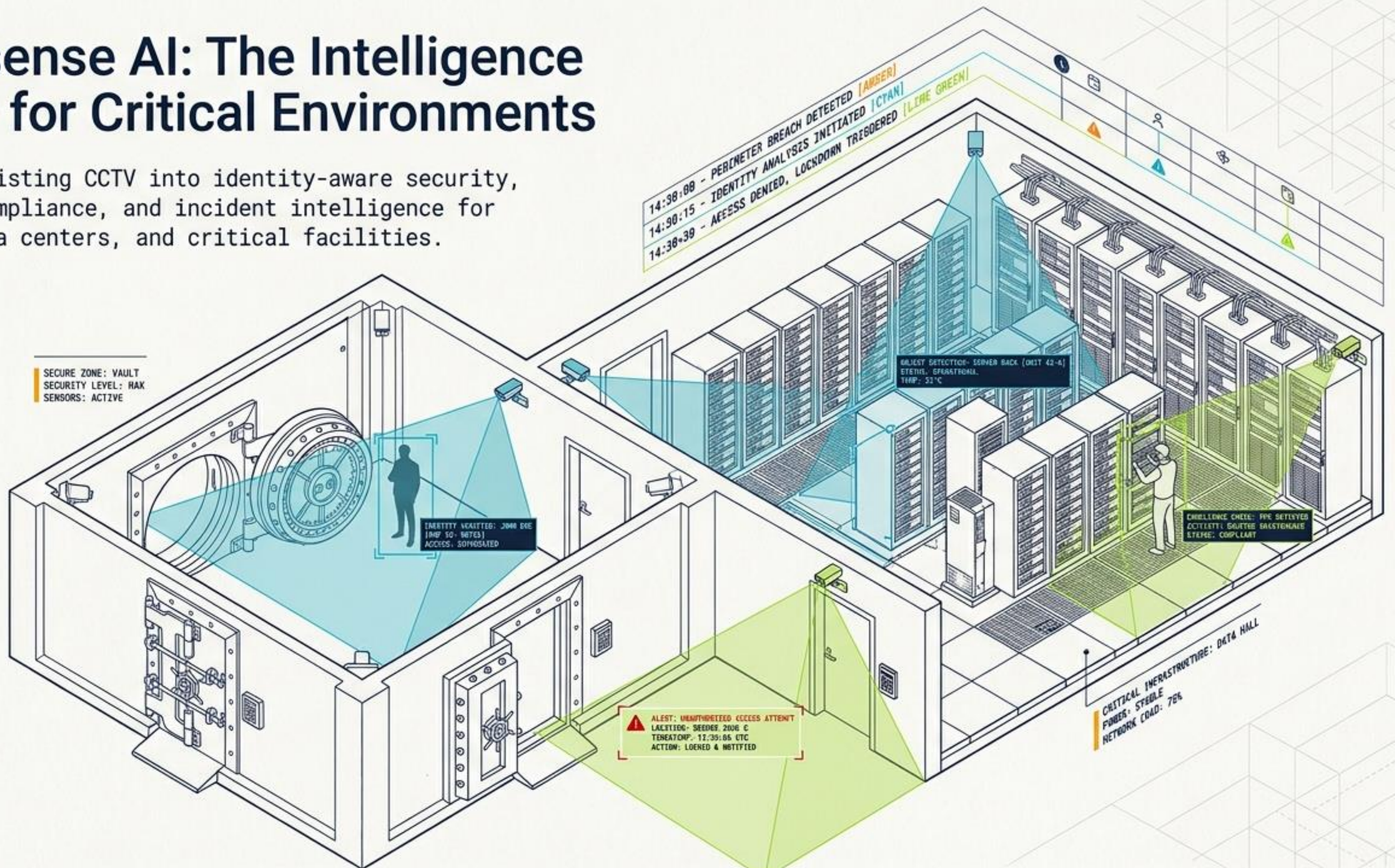


Camsense AI: The Intelligence Layer for Critical Environments

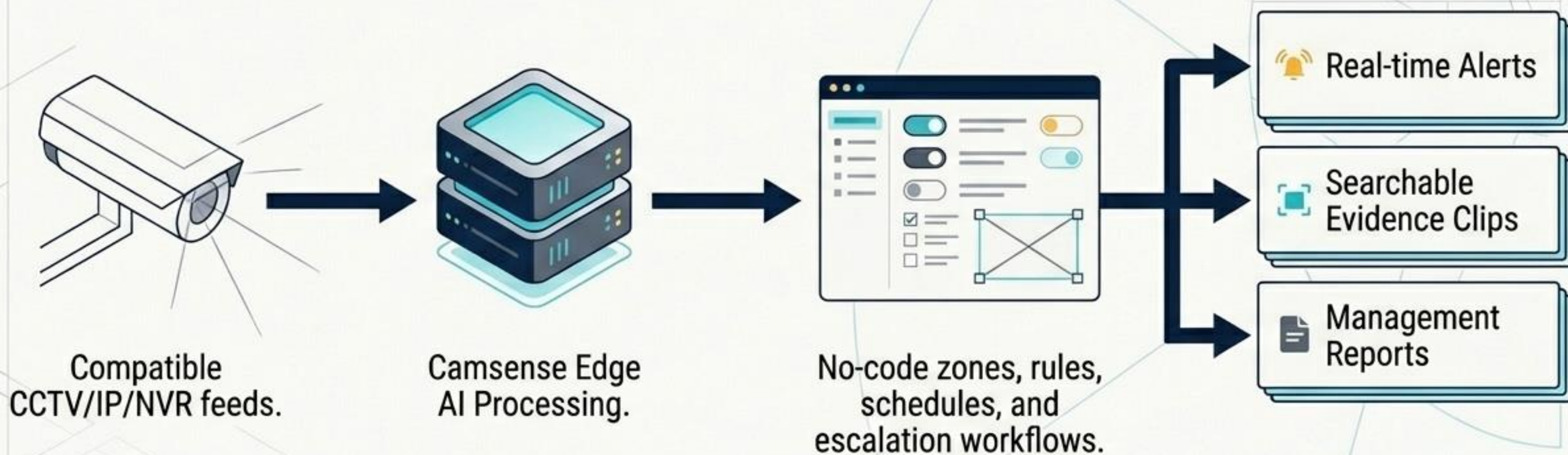
Turning existing CCTV into identity-aware security, access, compliance, and incident intelligence for banks, data centers, and critical facilities.



The Limit of Passive Recording vs. Active Intelligence

	Passive NVR (Status Quo)	Camsense Active Intelligence
MONITORING	✗ Security teams manually watch multiple gates, vaults, and racks.	✓ Automated real-time alerts for access exceptions and tailgating.
INCIDENT INVESTIGATION	✗ Slow, manual video review hours or days later.	✓ Instant, searchable history by identity, zone, and timestamp.
COMPLIANCE & AUDIT	✗ Unstructured video footage lacking context.	✓ Auditable logs, structured evidence clips, and policy-backed visibility.
INFRASTRUCTURE	✗ Expensive rip-and-replace required to upgrade.	✓ Connects directly to existing compatible CCTV/IP/NVR/RTSP feeds.

The Camsense Transformation Flow



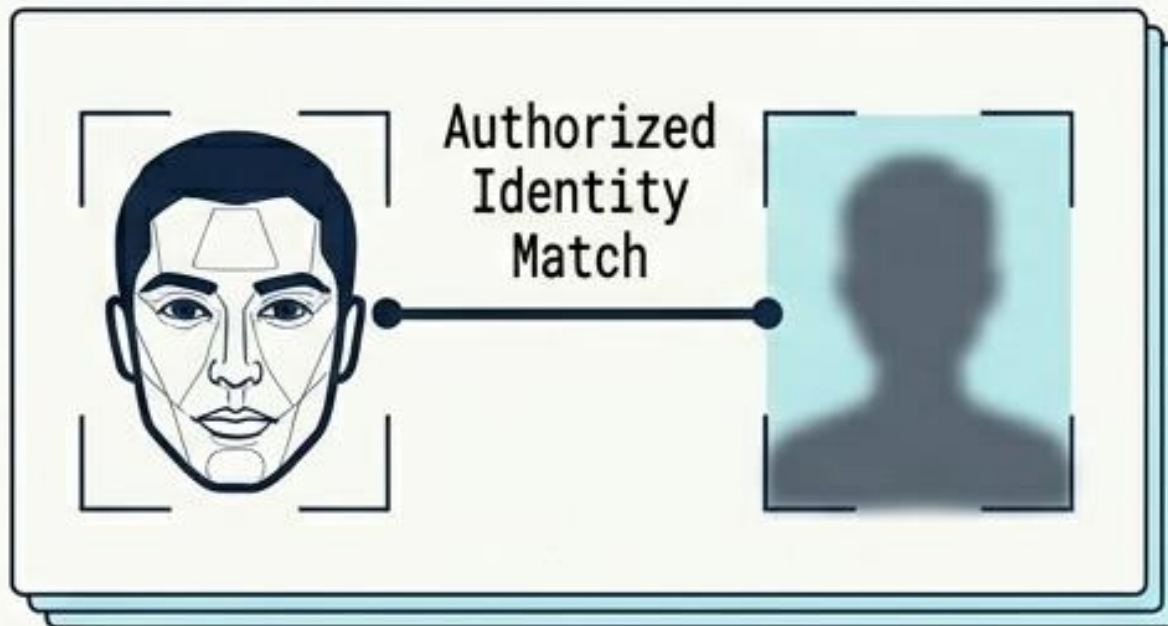
Connect existing camera feeds to generate real-time AI rules, identity events, and restricted-area policies—without replacing the full camera system.

The Capability Grid: Vertical-Specific Intelligence

	Bank Branches & Offices	Data Centers	Critical Facilities
Facial Recognition	✔ Teller verification, Vault access	✔ NOC & Server hall authorized entry	✔ Control room visibility
ANPR & Vehicles	✔ Cash van logs	✔ Vendor/Engineer gate access	✔ Perimeter logs & loading bays
Tailgating & Intrusion	✔ Vaults/Locker rooms	✔ Mantraps & Turnstiles	✔ After-hours perimeter
Queue & Crowd	✔ Customer lobby	(Not Applicable)	✔ Gate congestion
Loitering & Suspicious Dwell	✔ ATM Lobby	✔ Rack aisles & cages	✔ Sensitive equipment zones

Identity Intelligence Governed by Strict Policy

Capability (Use Cases)

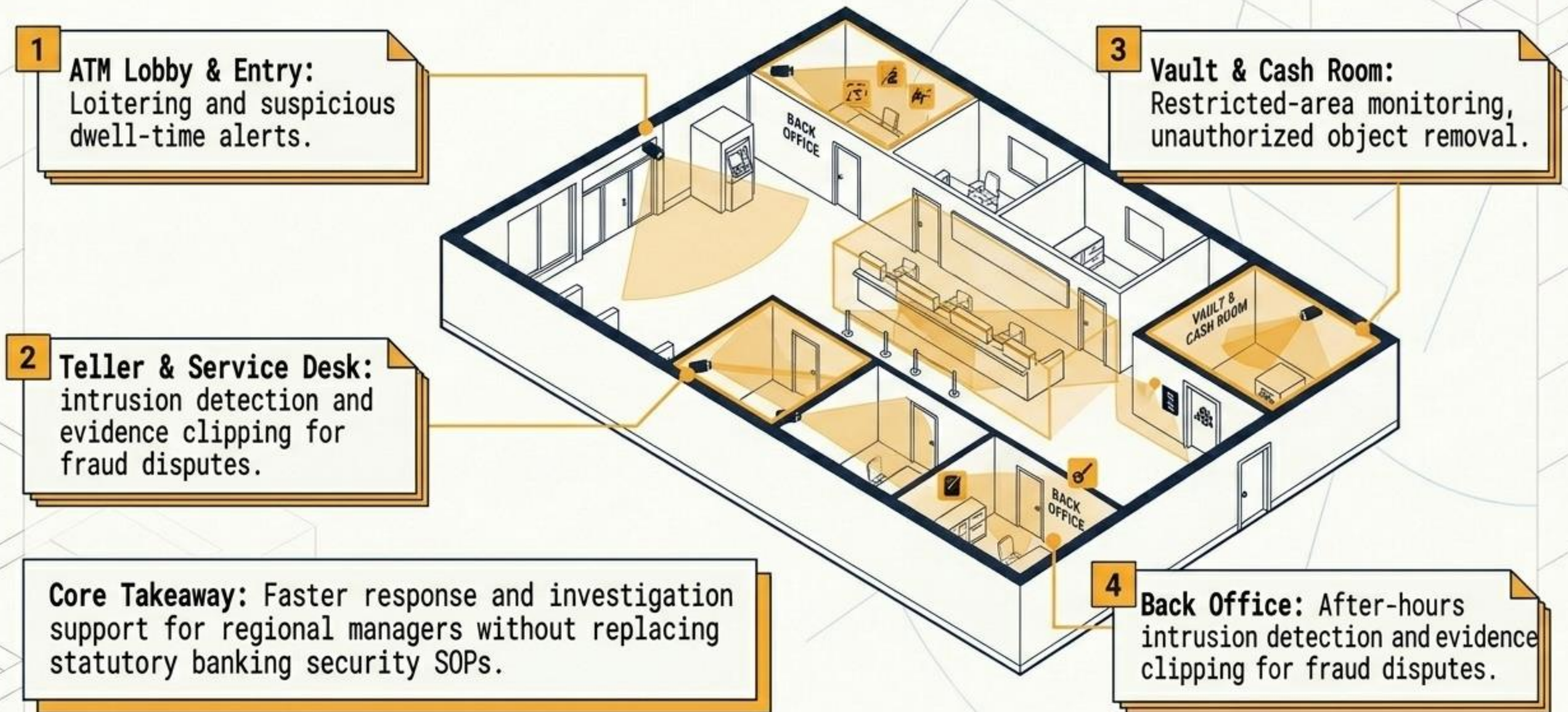


- Authorized staff entry/exit logs.
- VIP/Auditor/Vendor pre-approved recognition.
- Watchlist alerts for banned/terminated individuals.
- Unknown-person alerts in vaults and NOCs.

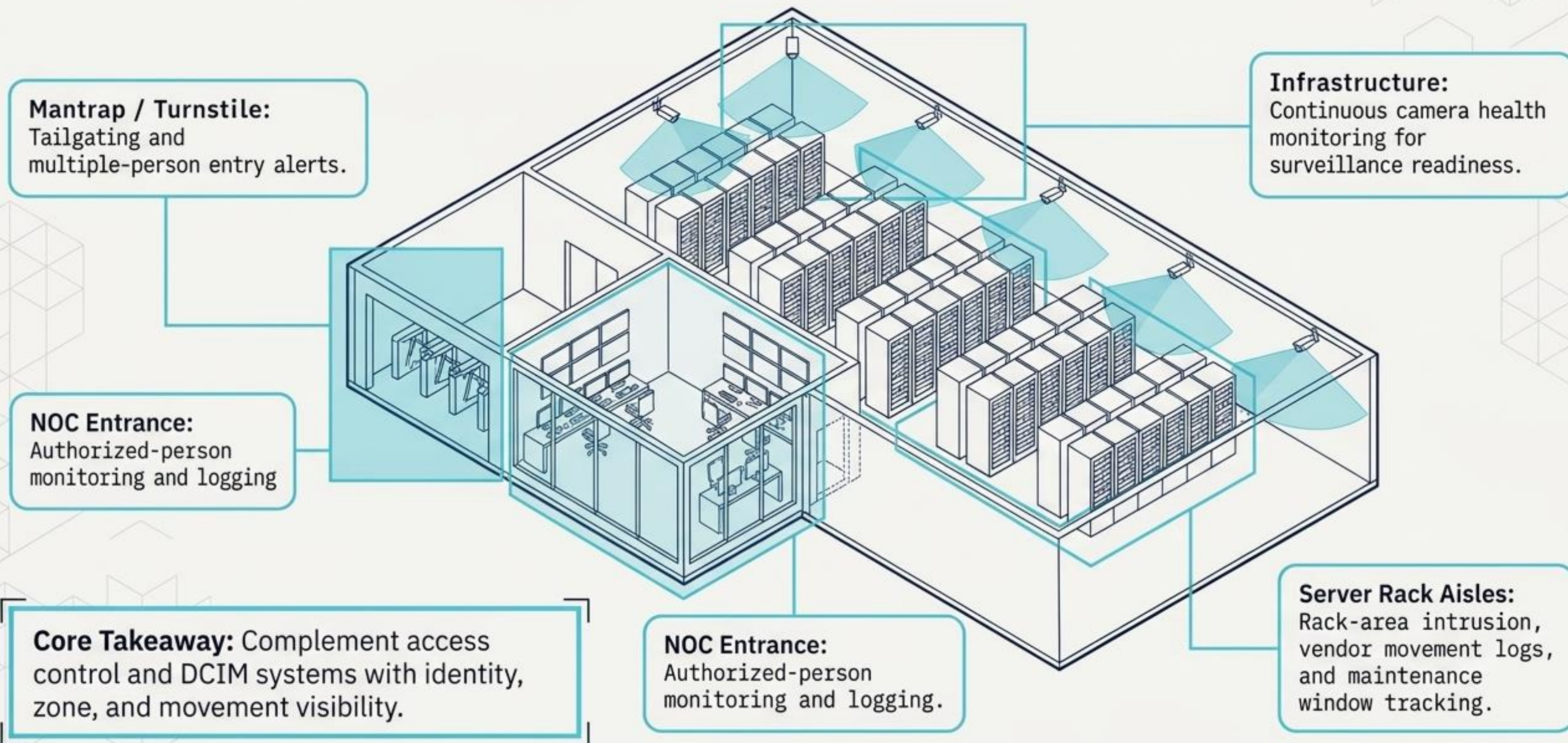
The Identity & Governance Guardrails Table

- ✓ **Consent & Enrollment:** Biometric matching requires explicit legal/compliance approval and enrollment.
- ✓ **Role-Based Access (RBAC):** Alerts restricted to authorized security/management only.
- ✓ **Data Lifecycle:** Strict retention limits and audit trails for all searches.
- ✓ **Physical Signage:** Visible notices required in all monitored zones.

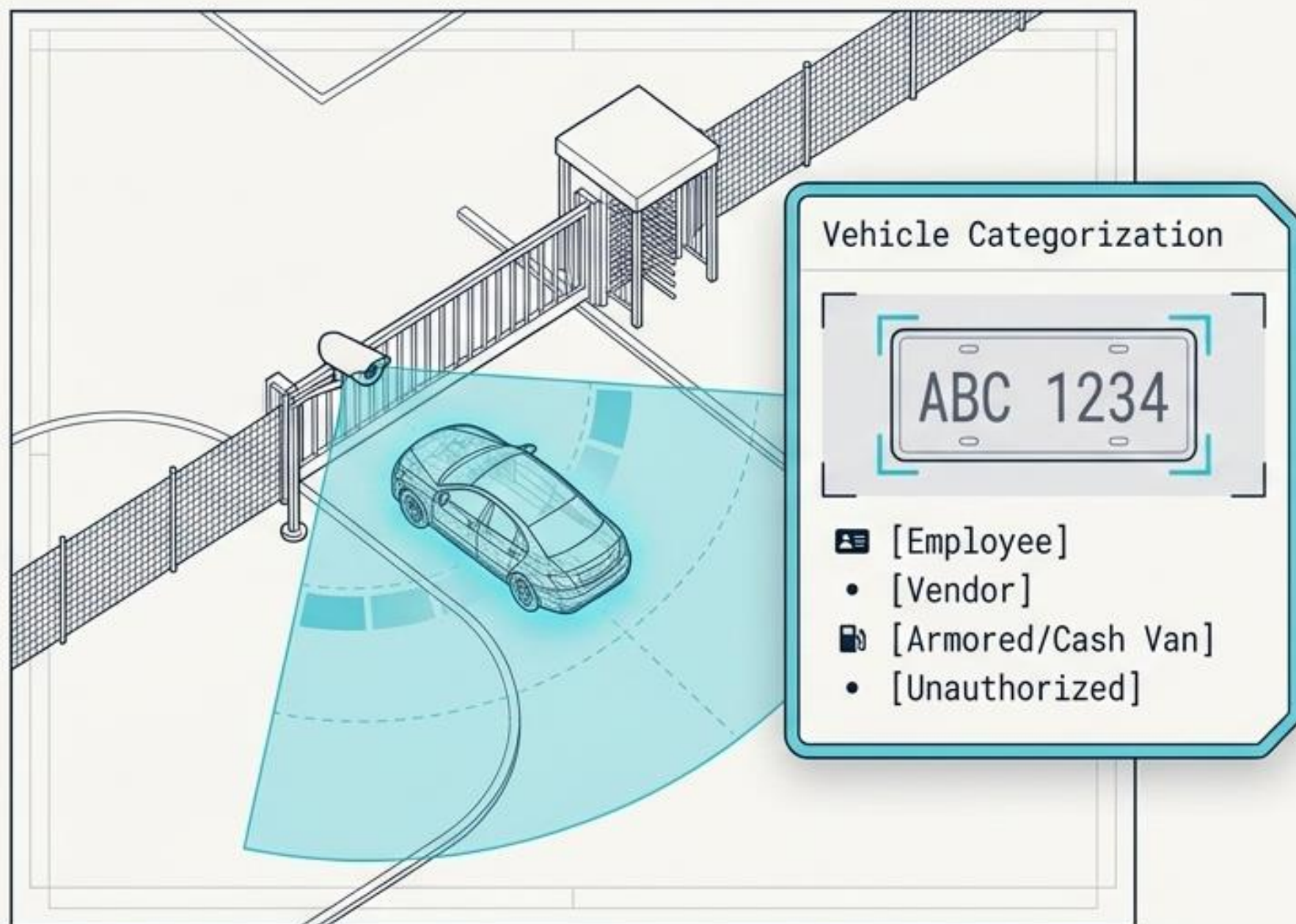
Branch Intelligence: Beyond Passive Recording



Data Center Security: Rack-Level Accountability



Critical Facilities & Automated Gate Operations



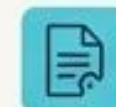
Perimeter intrusion and service-entry monitoring.



Wrong-parking and restricted-bay alerts.



Visual fire/smoke detection alerts (complementary layer).

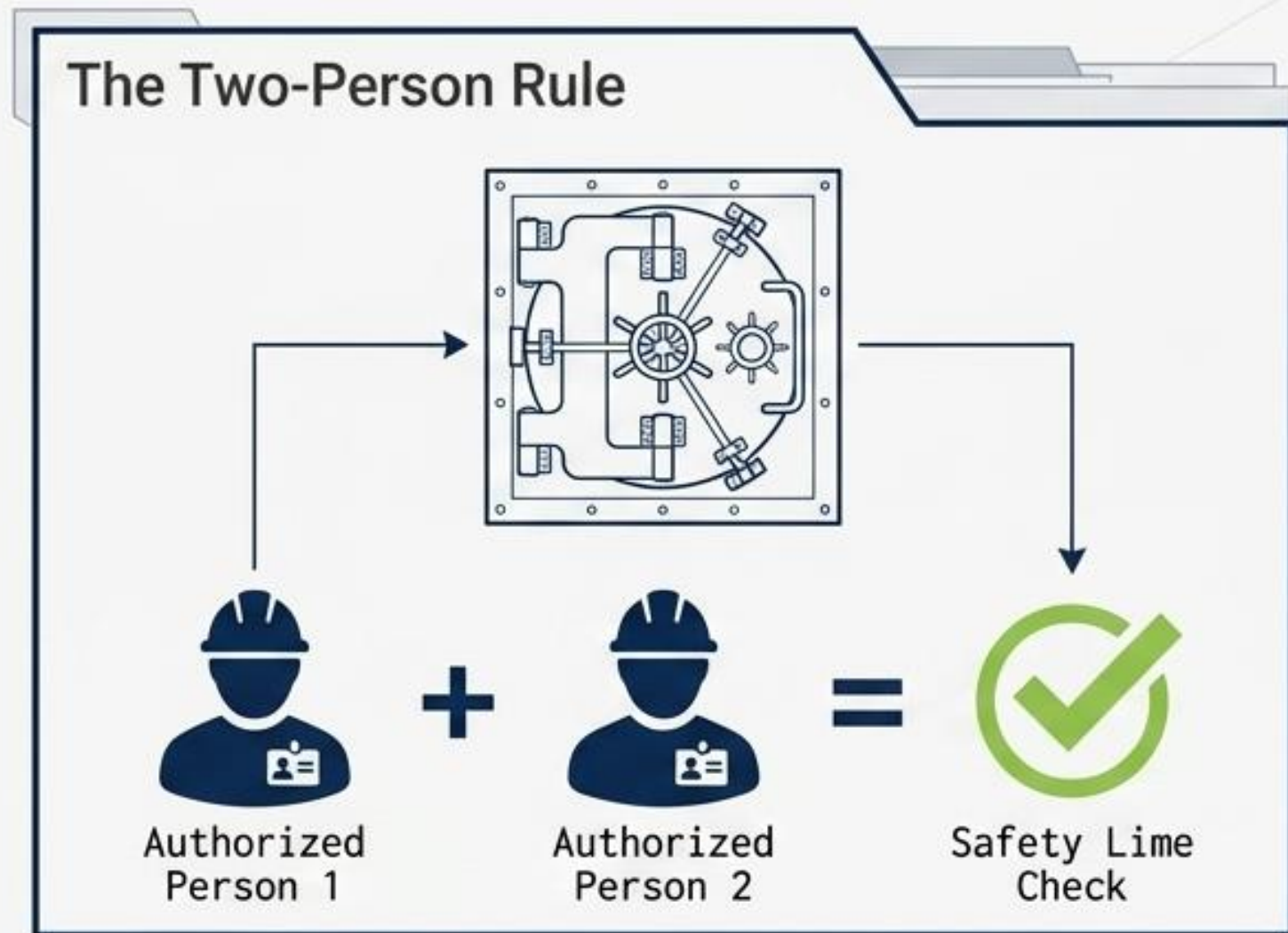


Loading bay and gate congestion reports for operational planning.

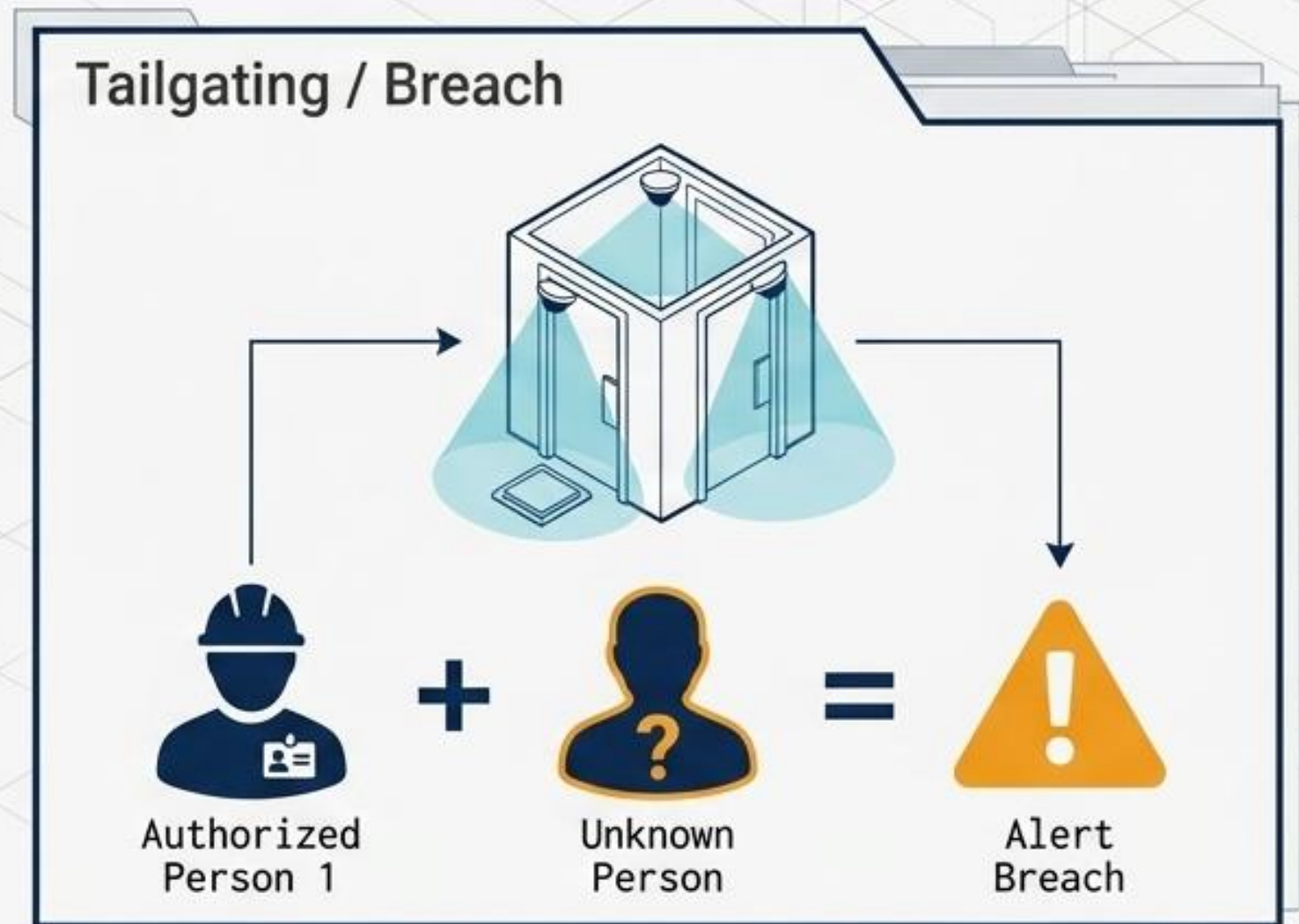
Note: ANPR requires plate-facing camera angles, appropriate lighting, and database integration.

The Logic of Secure Access: Correlating Events

The access system says a card was used; camera intelligence proves who actually walked through.

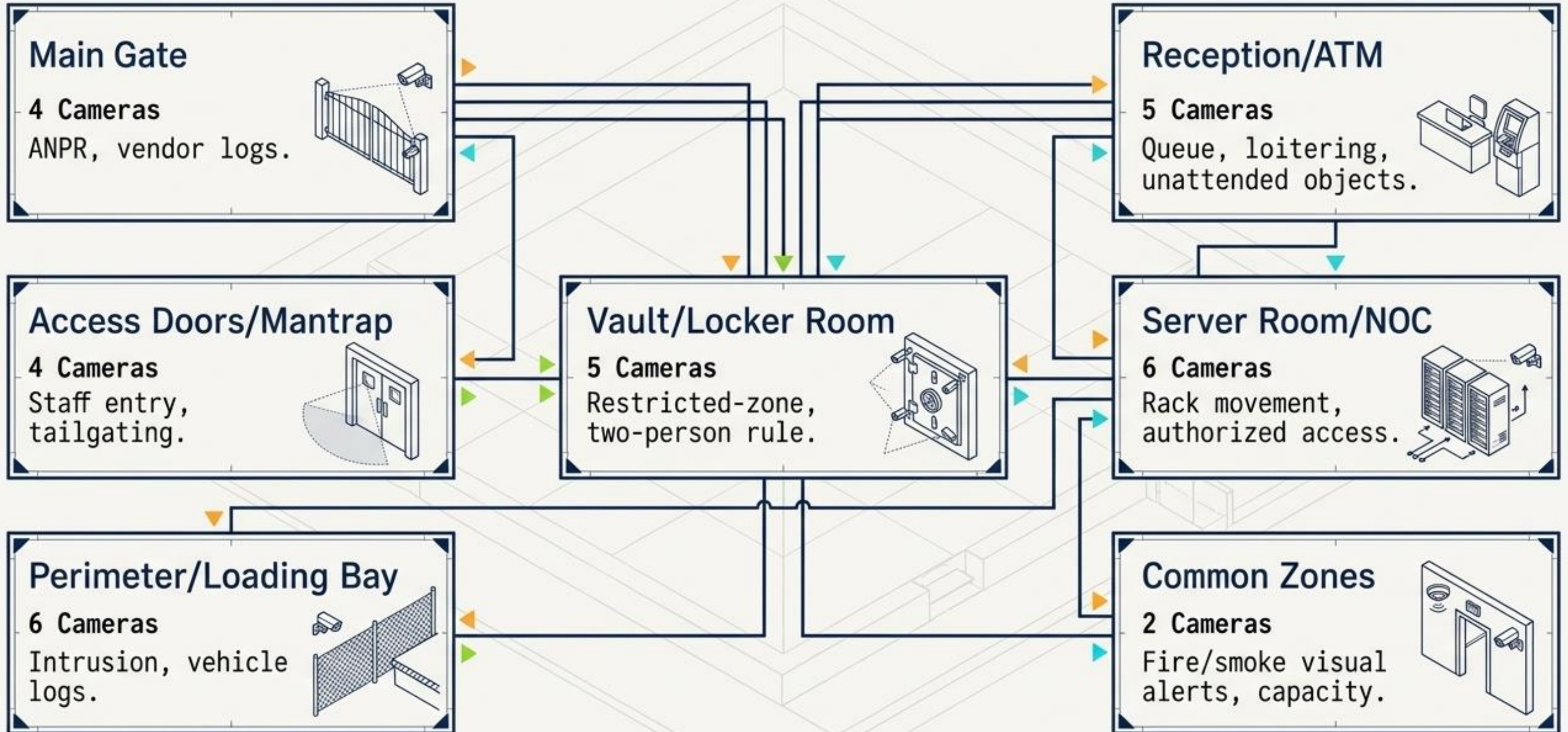


Correlating multiple identities in a single frame to ensure compliance in vaults, cash rooms, and critical operations areas.



Cross-referencing badge-access logs with situational camera awareness at mantraps and secure corridors.

The Spatial Blueprint: A 32-Camera Deployment



The Command Dashboard: Video as a Searchable Database

Context: [Timestamp] + [Camera Zone] + [Severity Level].

The Alert Anatomy UI

Intelligence: [Event Type: Tailgating] + [Identity Metadata].

The screenshot displays the Camsense interface for a specific alert. At the top, a yellow banner shows the context: [2024-05-17 14:23:05 UTC] + [Vault Entrance Cam 01] + [CRITICAL]. Below this, the alert details are listed: EVENT: TAILGATING_BREACH, CONFIDENCE: 98.5%, and IDENTITIES DETECTED: [ID: STAFF_004, BADGE: AUTHORIZED, ROLE: MANAGER] and [ID: UNKNOWN_02, BADGE: NONE, ROLE: ALERT]. ATTRIBUTES: [OBJECTS: BACKPACK, HARD_HAT]. The central video player shows a scene with two individuals: [PERSON 1: AUTHORIZED] and [PERSON 2: UNKNOWN], with an [ALERT: TAILGATING] notification. A play button is overlaid on the video. A timeline at the bottom indicates the clip duration: [14:23:05 - 14:23:15].

Evidence: [Auto-generated Video- Evidence Clip].

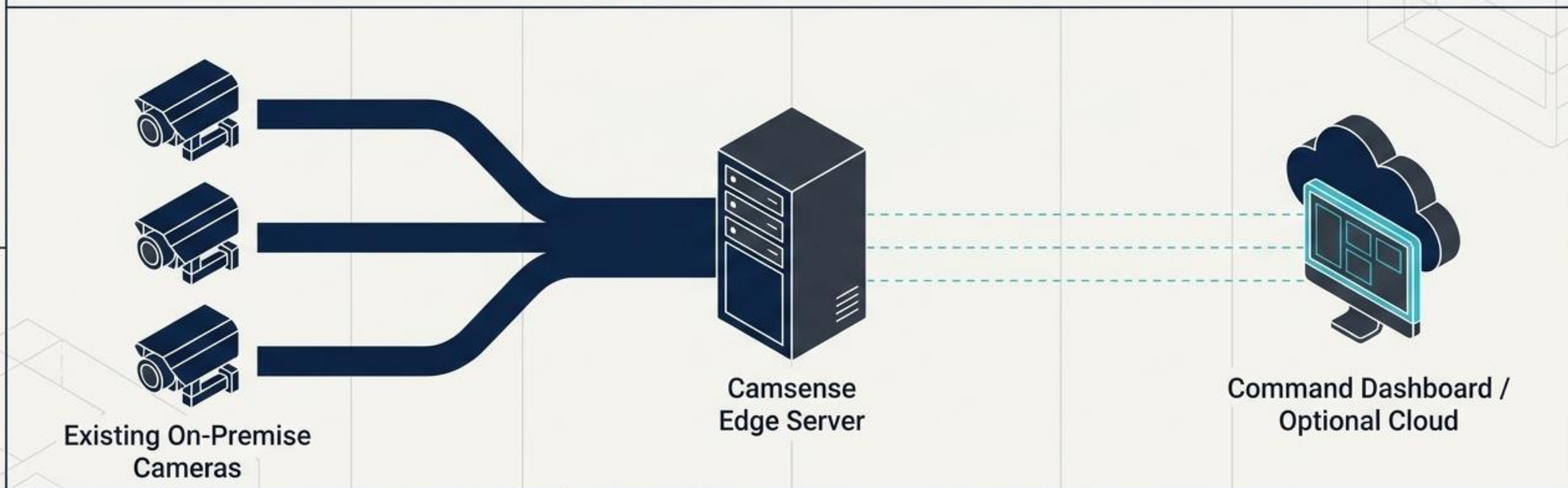
Traceable operational records.

Searchable history by person, vehicle, date, and zone.

Daily/weekly reports customized via Role-Based Access for CISOs, Branch Managers, and Control Rooms.

Edge-First Architecture: Low Bandwidth, High Privacy

The Edge-First Architecture Diagram



Video streams are processed locally on-premise.

Internet/Cloud is strictly for sync, lightweight notifications, and remote support.

Hardware sizing is customized based on camera count, resolution, FPS, and concurrent streams following technical validation.

Responsible AI: Security and Privacy by Design



Purpose-Built

CCTV + AI is strictly for declared security, safety, compliance, and operations.



Zone Exclusions

Absolute prohibition of analytics in private/sensitive spaces (washrooms, changing rooms, prayer rooms).



Data Security

Enforced secure connectivity, continuous access reviews, structured data retention retention controls, and total alignment with enterprise incident-response SOPs.

Business Impact & Commercial Model

Incident Lifecycle Timeline

Manual Review Workflow

Incident Detected

Manual Retrieval

Review & Analysis

Report Generation

Closure

Hours/Days

Camsense Automated Workflow

Automated Detection & Alerting

Instant Retrieval

Automated Reporting

Seconds/Minutes

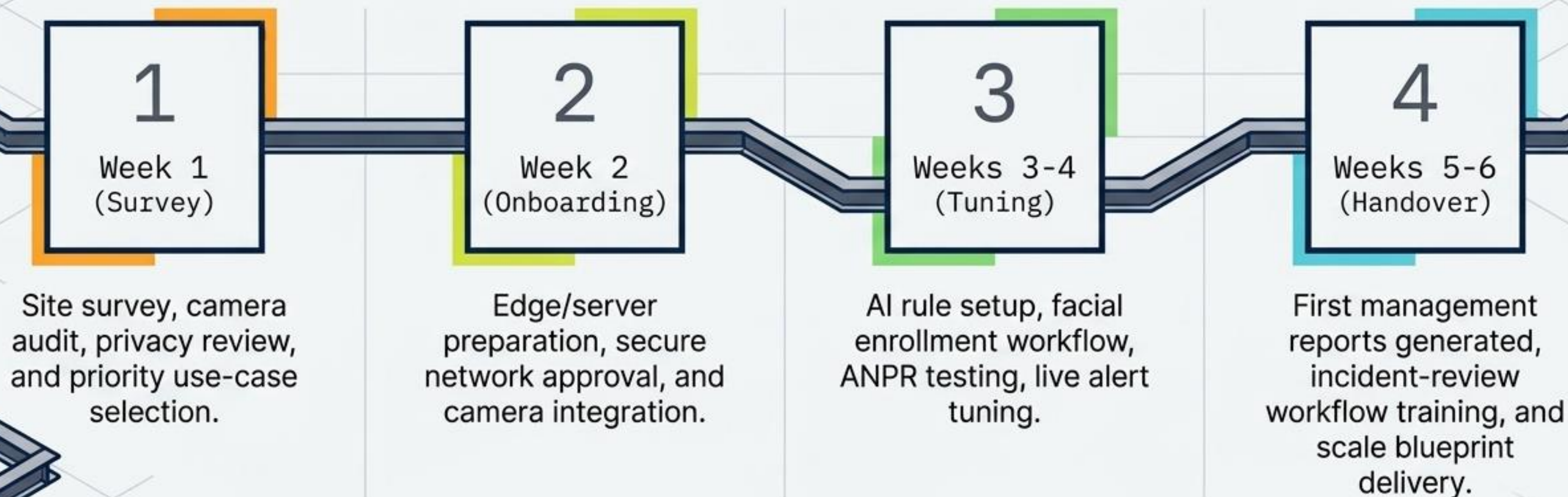
Faster incident investigation, reduced manual review time, and scalable governance.

Commercials Box

Commercials & Ownership Model

- **Ownership-friendly model:** One-time software license (based on scoped cameras) + Annual AMC from Year 2.
- **No heavy SaaS by default.** Edge hardware/GPU billed at actuals.
- Final quote generated only after a thorough camera list, site survey, and IT/security validation.

The 30–45 Day Pilot: Validate Value Quickly



Recommended Next Step: Select 10–20 priority cameras (e.g., Main Gate, Mantrap, Vault, Server Room) to begin the technical readiness survey.