



JARVIS
Powered by Staqu

We've Been Using CCTV the Wrong Way in Our Buildings for 30 Years



Here's What It Was Actually Supposed to Secure

A data-backed playbook for CEOs who want to turn their existing camera infrastructure into a revenue engine.



Fire
Detection



Perimeter
Security



Crowd
Detection



Left
Baggage



Smart
Parking



Intrusion
Detection

A Note Before You Begin

This is not a vendor pitch. There is no technology agenda hiding behind a statistic. What this is, is a reckoning, for every manufacturing business that has spent decades installing cameras across its plant floor and used them exclusively to watch for thieves.

What your cameras have actually been watching, the near-miss that preceded last month's accident, the material that left through Gate 3 during shift changeover, the machine that gave you 6 hours of warning before it broke down, the PPE violation that happened at 2 AM when the supervisor was on the other side of the floor, none of that has ever been brought to you. Because nobody built the intelligence to read it.

Read this book with a digital highlighter. Share it with your Safety Head, your CFO, your Plant Operations Manager. And then, this week, do something that is long overdue: ask your plant what it already knows.

— The JARVIS Intelligence Team, Staqu Technologies



04

Chapter 1

You Have 200 Cameras But Your Perimeter Was Still Breached Last Tuesday

07

Chapter 2

Your Parking Structure Is Your Most Expensive Blind Spot.

09

Chapter 3

The Crowd Became Dangerous 9 Minutes Before Anyone Noticed.

11

Chapter 4

The Visitor Logged In, The System Logged Out But Nobody Tracked What Happened In Between.

14

Chapter 5

Your Security Budget Is Paying for Guards to Watch Cameras That Are Already Watching Everything.

16

Chapter 6

Fire, Smoke, Abandoned Objects: The 3 Alerts That Save Lives and Nobody Has Turned On.

19

Chapter 7

They Didn't Add a Single Guard. They Just Finally Made Their Cameras Intelligent.

You Have 200 Cameras But Your Perimeter Was Still Breached Last Tuesday



CHAPTER

1

Every Grade A office park, mall, mixed-use development, and large infrastructure facility in India has a perimeter security system. Cameras at every gate. Guards at every entrance. Access control at every door. And in almost every single one of them, a breach, an unauthorised vehicle entry, a tailgating event, a person accessing a restricted zone, is detected not by the system, but by a guard who happened to be looking at the right screen at the right time. Or not at all, until the incident log is reviewed the next morning. The cameras are not the problem. The problem is that the cameras are recording and nobody has built the intelligence to read what they see in real time.

The Perimeter Security Paradox

The average Grade A office campus or mall in India has between 80 and 300 CCTV cameras. The average security operations centre monitoring those cameras has between 2 and 6 staff on any given shift. Basic mathematics: at 200 cameras, each guard would need to monitor 33 to 100 feeds simultaneously to achieve full coverage. That is not surveillance. That is the appearance of surveillance.

“ The illusion of security is more dangerous than the absence of security. One makes you feel protected. The other makes you act. ”



What Your Perimeter Is Currently Missing

- Unauthorised vehicle entry: Guard checks at gate, misses tailgating, cloned plates, after-hours entry when guard is elsewhere
- Perimeter fence breach: Patrol walkround or post-incident review, average detection lag: 4 to 18 hours
- Loitering near sensitive zones: Guard observation, missed entirely during shift overlaps and low-visibility hours
- After-hours person entry: Access card logs, does not detect physical bypass, door-holding, or unregistered entry
- Vehicle left in no-parking zone: Manual patrol, average detection: 45 to 120 minutes
- Suspicious perimeter behaviour: Reactive, detected only after escalation, not before

What JARVIS Perimeter Intelligence Does



35% reduction in manual security costs through JARVIS perimeter automation, replacing reactive guard observation with proactive AI alerting.



99.9% detection accuracy for perimeter breach events, the JARVIS infrastructure benchmark across all deployments.



< 30 sec average time from perimeter breach detection to security team alert vs. 4 to 18 hours under traditional monitoring.

YOUR MOVE THIS WEEK:

Identify your 3 highest-risk perimeter points, historically, by incident frequency or blind spot location. Ask: is each one covered by a camera? Is that camera generating real-time alerts? If not, it is decoration.



Your Parking Structure Is Your Most Expensive Blind Spot

CHAPTER

2

Infrastructure facilities spend heavily on parking. The construction cost of a covered parking bay in a Grade A development in India ranges from ₹3 lakh to ₹8 lakh per bay. The operational cost: lighting, ventilation, maintenance, security, adds another ₹12,000 to ₹24,000 per bay per year. And in most facilities, the return on that investment is measured by one metric: whether the parking is full.

Nobody is measuring how long vehicles stay. How many bays are permanently occupied by staff vehicles that should be in a designated zone. How many vehicles enter the visitor section and never log out. How many parking violations, wrong zones, fire lane blockages, reserved bay misuse are occurring daily. How long the average visitor spends searching for a bay, and how that experience affects their perception of your facility.

The parking structure is one of the most camera-dense areas in any infrastructure facility. It is also one of the least intelligently monitored.

The Parking Intelligence Gap: What Most Facilities Don't Measure

- Average vehicle dwell time by zone and time of day
- Occupancy rate by bay type: visitor, staff, reserved, accessible in real time
- Unauthorised zone parking: staff in visitor bays, vehicles in fire lanes
- Entry-exit time mismatches: vehicles logged in but not out, or out without a logged entry
- Peak demand windows: when does parking hit capacity, and how far in advance can it be predicted?
- Visitor parking conversion: what percentage of visitors who park actually enter the facility?

What Smart Parking Intelligence Delivers

JARVIS smart parking management uses existing parking structure cameras to generate continuous operational intelligence across every bay and every zone. The system does not require new sensors in the bays, new signage, or any physical infrastructure change. It reads the cameras that are already installed.



30% reduction in operational costs through parking occupancy analytics and zone management, JARVIS infrastructure benchmark.

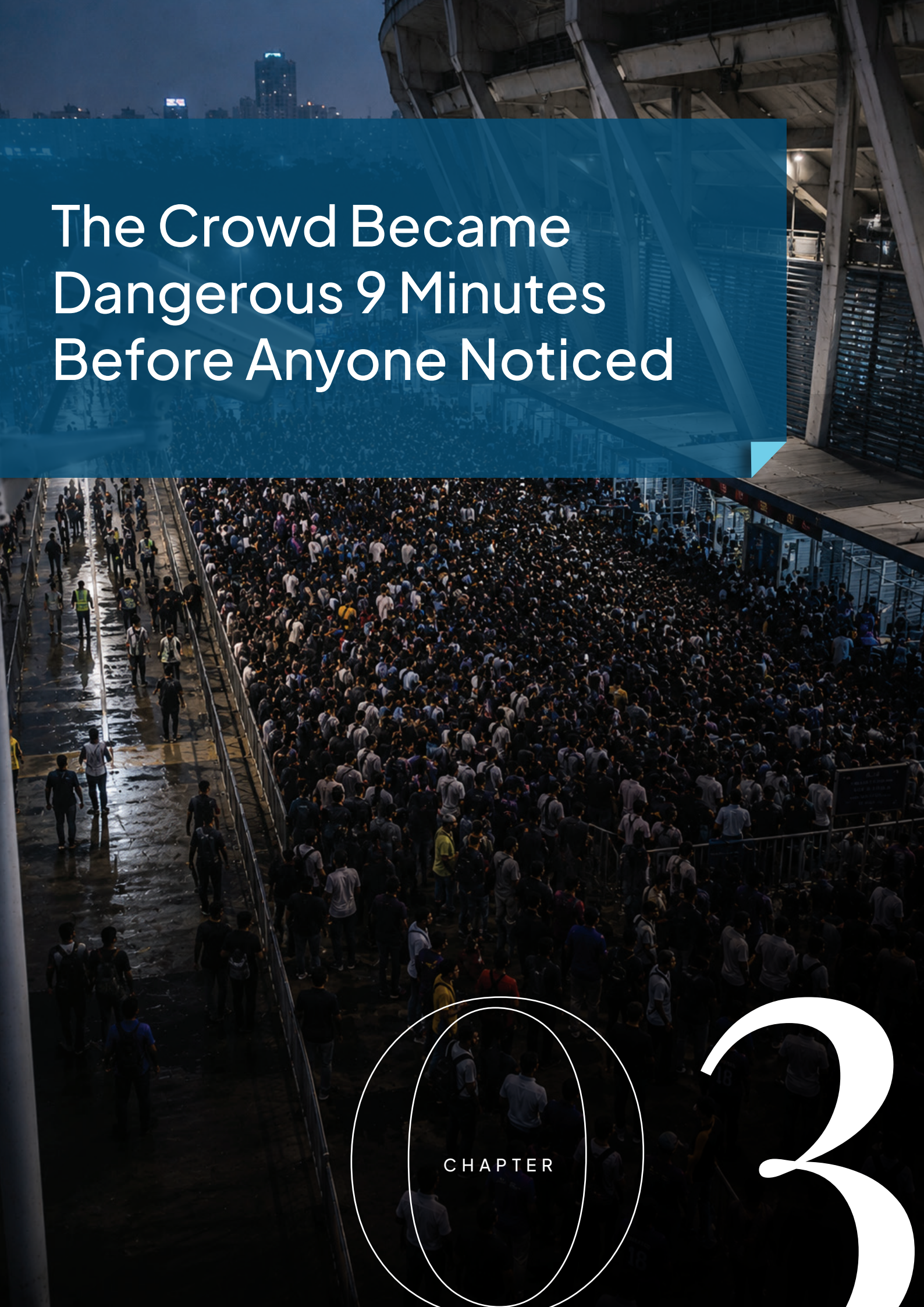


20% improvement in asset tracking and protection through automated vehicle logging and zone violation detection.



₹18–45L estimated annual revenue leakage in a 500-bay paid parking facility from unlogged overstays and zone misuse.



A large crowd of people is gathered on a bridge at night. The crowd is dense, filling the bridge deck. In the background, a city skyline is visible with several lit-up buildings. The bridge has a metal railing on the left side. The overall scene is dimly lit, with the city lights providing the main source of illumination.

The Crowd Became Dangerous 9 Minutes Before Anyone Noticed

CHAPTER

3

Saturday evening at a large mall in Delhi. A popular store's closing sale has drawn a larger crowd than expected. By 6:30 PM, the crowd at the ground floor entrance has reached a density that trained safety professionals would classify as a serious crush risk.

The CCTV cameras above the entrance have been watching the crowd build since 6:21 PM. No alert has been triggered. The security guard at the door is managing individual entry. The control room operator is watching 48 other feeds.

At 6:39 PM, a pushing incident injures 3 visitors. The investigation will later show that every warning signal was visible on camera 9 minutes before the incident.

Crowd intelligence is not a luxury for large infrastructure facilities. It is a safety obligation and in India, where public space events, festivals, and retail peaks routinely create crowd conditions, it is one that most facilities are systematically failing to meet.

The Crowd Safety Numbers Indian Infrastructure Cannot Ignore

- 79 people died in the Hathras stampede, 2024: a crowd management failure at a public gathering.
- 4 min the average time between crowd reaching dangerous density and an incident occurring in documented crush events globally. (Fruin Crowd Safety Research)
- 9 min the average lead time JARVIS crowd intelligence generates before density reaches critical threshold, giving facilities a 5–minute intervention window.

How Crowd Intelligence Works

JARVIS crowd analytics uses existing overhead cameras to count people in any defined zone in real time: a lobby, an entrance corridor, a food court, a concourse, a stairwell. The system tracks not just how many people are present but how fast the density is increasing and what direction the crowd is moving.

When density in any zone approaches a predefined threshold, set based on the zone's safe occupancy capacity, JARVIS triggers an alert to the control room and, if configured, to floor security staff directly on their devices. The alert arrives before the situation becomes dangerous, not after.

JARVIS crowd intelligence has been deployed at RCB IPL matches at M. Chinnaswamy Stadium one of India's highest-density crowd environments, with 35,000+ spectators in a confined space. The same intelligence architecture is applicable to any infrastructure facility that experiences predictable or unpredictable crowd concentration.

The Visitor Logged In, The System Logged Out But Nobody Tracked What Happened In Between



VISITOR STATUS

INSIDE

CHECK OUT

DURATION

LAST UPDATE
09:15 AM

CHAPTER

4

Your visitor management system logs name, ID, host, and time of entry. The visitor gets a pass. The system shows them as 'inside.' And from that point, for the rest of their visit, they are completely invisible to your operations.

Where did they go? Did they access only the areas they were authorised for? Did they leave when their appointment ended? Did they go to floors or zones that their pass did not cover? Did they tailgate someone into a restricted corridor? Did they allow their visitor pass to be used by someone else?

Visitor management in most Indian infrastructure facilities is entry management. It has nothing to do with visitor intelligence.

The Visitor Intelligence Gap

- The average large office campus in India processes 500 to 2,000 visitor entries per day
- Standard visitor management tracks entry time and exit time, nothing in between
- Restricted zone access violations by visitors are detected in fewer than 12% of cases by traditional systems (ASSOCHAM India)
- Visitor passes are shared, cloned, or misused in an estimated 3–7% of all visitor entries in large facilities
- Post-visit audit, confirming a visitor only accessed authorised areas, is impossible with traditional visitor management.



What AI-Powered Visitor Intelligence Ads

JARVIS visitor intelligence uses camera-based zone tracking to monitor visitor movement from entry to exit, not through biometric identification, but through pass-linked camera tracking and zone access correlation.



20% improvement in asset protection and tracking through JARVIS visitor intelligence vs. traditional entry-log-only systems.



< 12% of restricted zone access violations by visitors are detected by standard visitor management systems.



500–2,000 visitor entries processed per day in a large office campus or mall. Each one is currently invisible the moment they enter.

JARVIS IN ACTION

At a WeWork facility in a major Indian city, JARVIS visitor intelligence was deployed as part of a broader infrastructure security upgrade. Within the first 30 days, the system identified 14 instances of visitors accessing floors beyond their authorised level, 7 cases of visitor pass overstay beyond 3 hours with no exit log, and 3 cases of tailgating by visitors into tenant-restricted zones. All 24 events had been invisible under the previous system. The facility's visitor SOP was redesigned with JARVIS alert thresholds as the operational backbone.

Your Security Budget Is Paying for Guards to Watch Cameras That Are Already Watching Everything



CHAPTER

5

The average Grade A office campus or large mall in India spends between ₹1.2 crore and ₹4.5 crore per year on security operations, guards, supervisors, control room staff, and contract management overhead.

A significant proportion of that budget pays for people to watch camera feeds. To do manually, fallibly, and with inevitable attention gaps what an AI system can do continuously, simultaneously, and with **99.9% accuracy**.

This is not an argument for eliminating security staff. It is an argument for deploying them where human judgement, physical presence, and de-escalation capability actually matter and letting AI handle the part that requires eyes on 200 feeds at **3 AM**.

The Security Operations Cost Reality

35% reduction in manual security costs achievable through JARVIS automation of monitoring, alerting, and SOP enforcement.

20% reduction in monitoring inefficiencies: false alarms, missed events, delayed response, through AI-powered alert prioritisation.

₹1.2–4.5 Cr annual security operations spend in a Grade A office campus or large mall in India.

What JARVIS Frees Your Security Team to Do

- Respond to validated, real-time alerts, not monitor feeds hoping to catch something
- Manage physical de-escalation and crowd control, where human presence is irreplaceable
- Conduct directed patrols to zones flagged by AI as anomalous, not random walkrounds
- Focus on visitor and contractor management, the human interaction layer
- Handle emergency response, where speed and judgement matter, not screen-watching

What JARVIS Frees Your Security Team to Do

JARVIS enables a single security operations centre to monitor multiple sites, office parks, malls, mixed-use developments, from one dashboard. This is the shift from site-level reactive monitoring to portfolio-level proactive intelligence.

Fire, Smoke, Abandoned Objects: The 3 Alerts That Save Lives and Nobody Has Turned On



CHAPTER

6

Three categories of safety events account for the majority of life-safety incidents in large infrastructure facilities: fire and smoke, abandoned or suspicious objects, and crowd crush. All three are detectable by camera, significantly earlier than traditional sensor-based systems. All three are almost universally unmonitored by AI in Indian infrastructure facilities today.

This is not a technology availability problem. The technology exists, is proven, and is already deployed in critical environments globally and in India. It is a deployment decision problem. And every day that decision is deferred, the risk accumulates.

Fire and Smoke Detection: The 8–Minute Gap

Traditional fire detection relies on heat sensors and smoke detectors. These systems trigger when the fire or smoke has already reached a defined physical threshold, a temperature level, a particle density. By the time the sensor triggers, the fire has been burning for between 3 and 12 minutes.

JARVIS visual fire and smoke detection works from the camera feed, detecting the visual signature of smoke or flame before it reaches sensor-trigger density. The average lead time gained is 8 to 12 minutes. In a large infrastructure facility, 8 minutes is the difference between a contained incident and a full building evacuation.

- 8–12 min earlier fire and smoke detection with JARVIS visual AI vs. traditional heat and smoke sensors.
- ₹15–80 Cr average insurance and rebuilding cost of a major fire incident in a Grade A commercial property in India. (GIC Re India data)
- 3 min average time for a fire to spread from ignition to a second room in a commercial building without early detection. (NFPA)



Abandoned Object Detection: The 22–Minute Window

An abandoned bag in a public space, a mall lobby, an airport terminal, a stadium concourse, is a security threat that requires immediate response. In most Indian infrastructure facilities, the detection method is a guard noticing it on a walkround or a member of the public reporting it.

The average time between an object being abandoned in a monitored public space and human detection in a traditional security setup is between 15 and 40 minutes. JARVIS abandoned object detection triggers an alert within 2 to 3 minutes of an object being left unattended in a defined zone, dramatically reducing the response window.

Hygiene Compliance Monitoring: The Standard Nobody Is Meeting

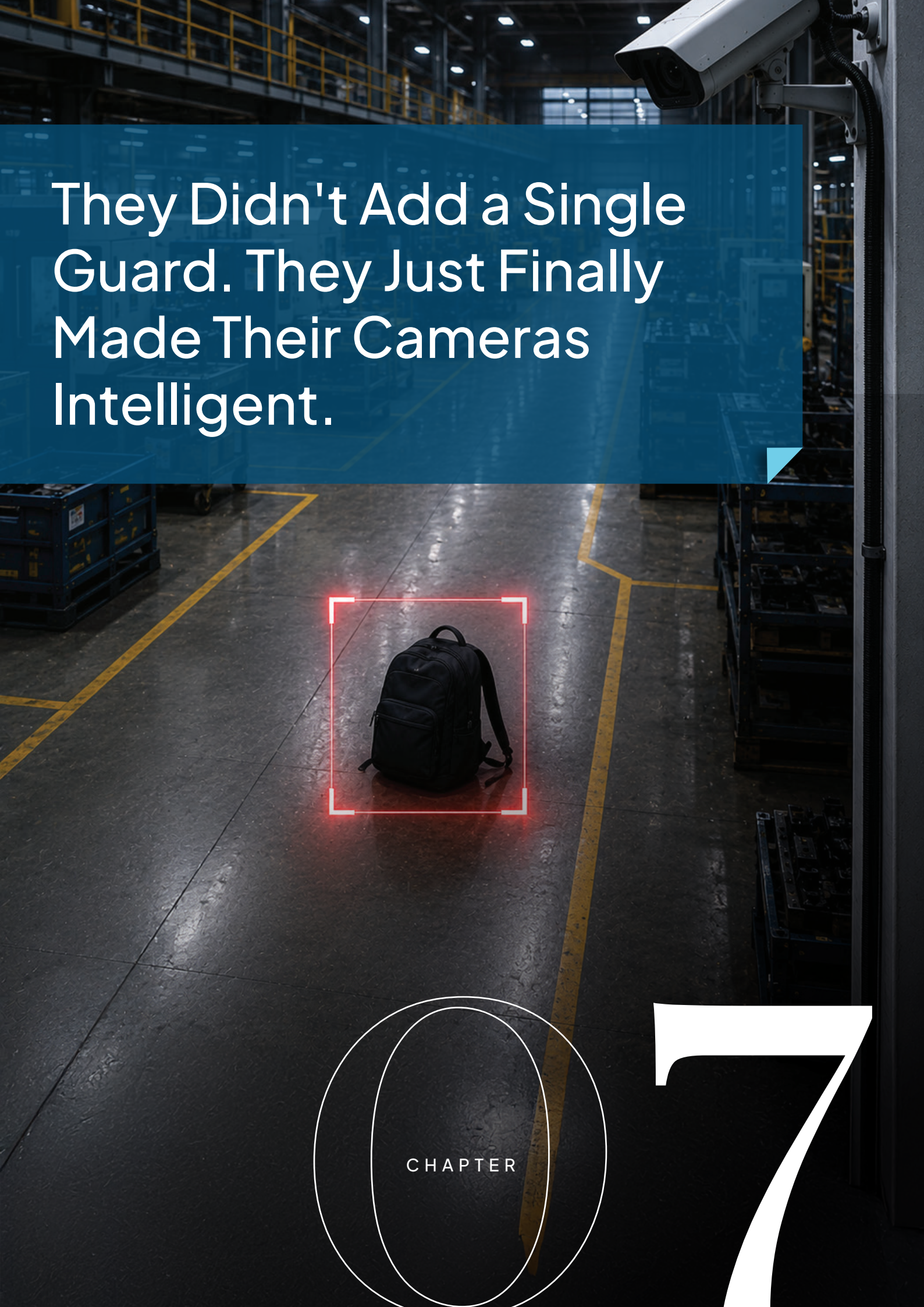
Post-COVID, hygiene compliance in public infrastructure spaces, handwashing stations, sanitiser dispensers, surface cleaning protocols, became a regulatory and reputational requirement. Most facilities added the infrastructure: dispensers, signage, cleaning schedules. Almost none of them added the monitoring.

JARVIS hygiene compliance monitoring uses camera analytics to detect handwashing behaviour at sinks, sanitiser dispenser usage at entry points, cleaning staff activity patterns, and cleanliness standard deviations in food courts and washrooms. The system generates compliance rates by zone and shift, giving facility managers the data to enforce standards rather than assume them.

- **67% of hygiene** compliance failures in large public facilities occur during the 3 hours of lowest staff supervision, late afternoon and post-closing. (WHO facility hygiene benchmarks)
- **34% of visitor** complaints in Grade A malls and office parks relate to hygiene and cleanliness standards, the single largest category of facility complaints. (ICSC India 2024)

THE SAFETY ALERT AUDIT:

Ask your safety team: in the last 12 months, how many fire or smoke events were detected by camera vs. by sensor? How many abandoned object incidents were detected proactively vs. reactively? If the answer to both is zero proactive, your safety system is entirely reactive.



They Didn't Add a Single
Guard. They Just Finally
Made Their Cameras
Intelligent.

CHAPTER

7

Everything in this book has been, until this chapter, a diagnosis. The perimeter that looks protected but is not. The parking structure that is full of data nobody is reading. The crowd that built to dangerous density before anyone noticed. The visitor who walked through your facility unsupervised. The security budget paying for people to do what AI already does better. The fire that the camera saw before the sensor did.

What the Playbook Means for Your Facility

The infrastructure sector has spent two decades investing in cameras and underspending on intelligence. The cameras are everywhere. They are recording everything. They are generating no operational value beyond the footage they passively store.

The **35%** security cost reduction, the zero major incidents, the **₹2.1 crore** value recovery, none of this required new hardware. It required one decision: to start reading what the cameras had already been seeing.

Every infrastructure facility has its own version of the perimeter breach that nobody logged, the crowd that built too fast, the visitor who went where they should not have, the fire that the camera saw before the sensor did. The specific numbers differ. The principle does not.

Ask the cameras what they know. Act on what they tell you. Measure the result. Repeat.

Get In Touch

info@staqu.com | www.staqu.com