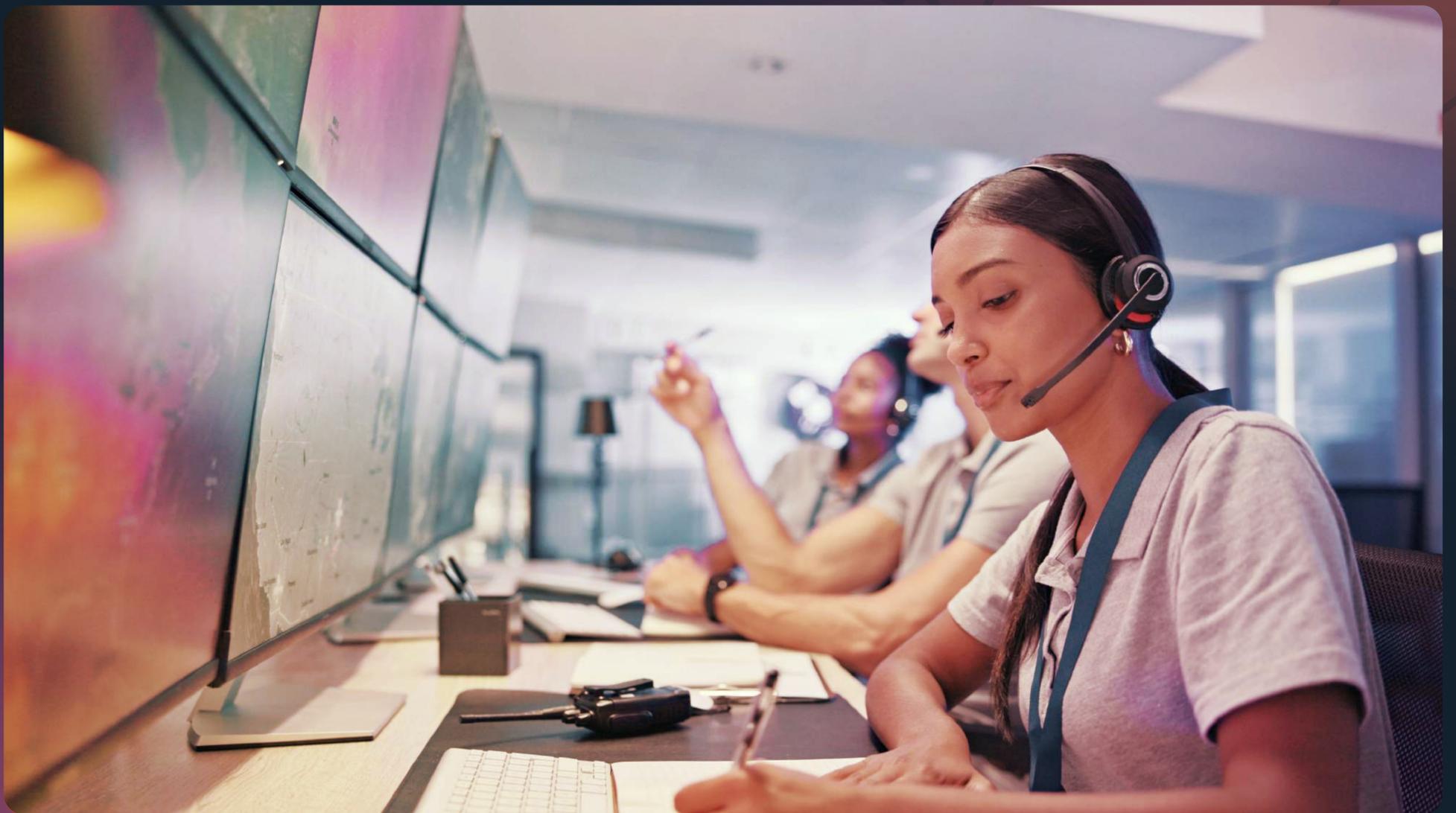




AURA

Always Safe



The ARC playbook

Closing the verified response gap by connecting alarm events to a vetted national network of security response partners, powered by smart tech.

The response model has changed

When an alarm activates, the expectation is simple: someone shows up.

For decades, the industry relied on police response or keyholding providers to fulfill that promise. Today, both models are under pressure: police response is limited, and many keyholding services are slow to arrive and often operate with little transparency.

In the UK, the **NPCC (National Police Chiefs' Council)** policy means police only respond to verified alarms, and even then, resources are under unprecedented strain. The result is a surge in unverified alarms going unanswered.

Alarm receiving centres (ARCs) are caught in the gap.

While video verification has improved credibility, it has also heightened expectations. When an incident is confirmed but no one attends, the ARC can carry the commercial and reputational fallout.



Private response is evolving to an integrated value layer.

Rather than managing fragmented suppliers or legacy response networks, forward-thinking ARCs are plugging into scalable security response infrastructure that strengthens their commercial offering without operational distraction.



Monitoring is measured on **outcomes**, not escalations

Historically, ARCs were evaluated on procedural performance: how fast an operator answered and how accurately they followed protocol. That is no longer enough.



“We’ve moved from alarm received, alarm closed - to alarm received, investigated, and resolved.”

— Adrian Meredith, Commercial Director at AURA

Modern commercial clients demand **certainty**. If an incident is verified, they expect a physical presence on-site. When attendance fails, the perceived value of the monitoring contract evaporates. The issue is not only whether someone attended, but whether the ARC can demonstrate exactly what happened, when it happened, and how it was managed.

“If you can’t answer those questions and you can’t evidence what happened, it doesn’t look great for our business either.”

— Rob Dovey, Managing Director at DSOC



Simply telling a customer that the police were notified – but may not attend – does not close the loop. In a commoditised market, “monitoring only” forces you into price conversations. Integrated response moves the discussion back to value.

The operational reality of manual coordination

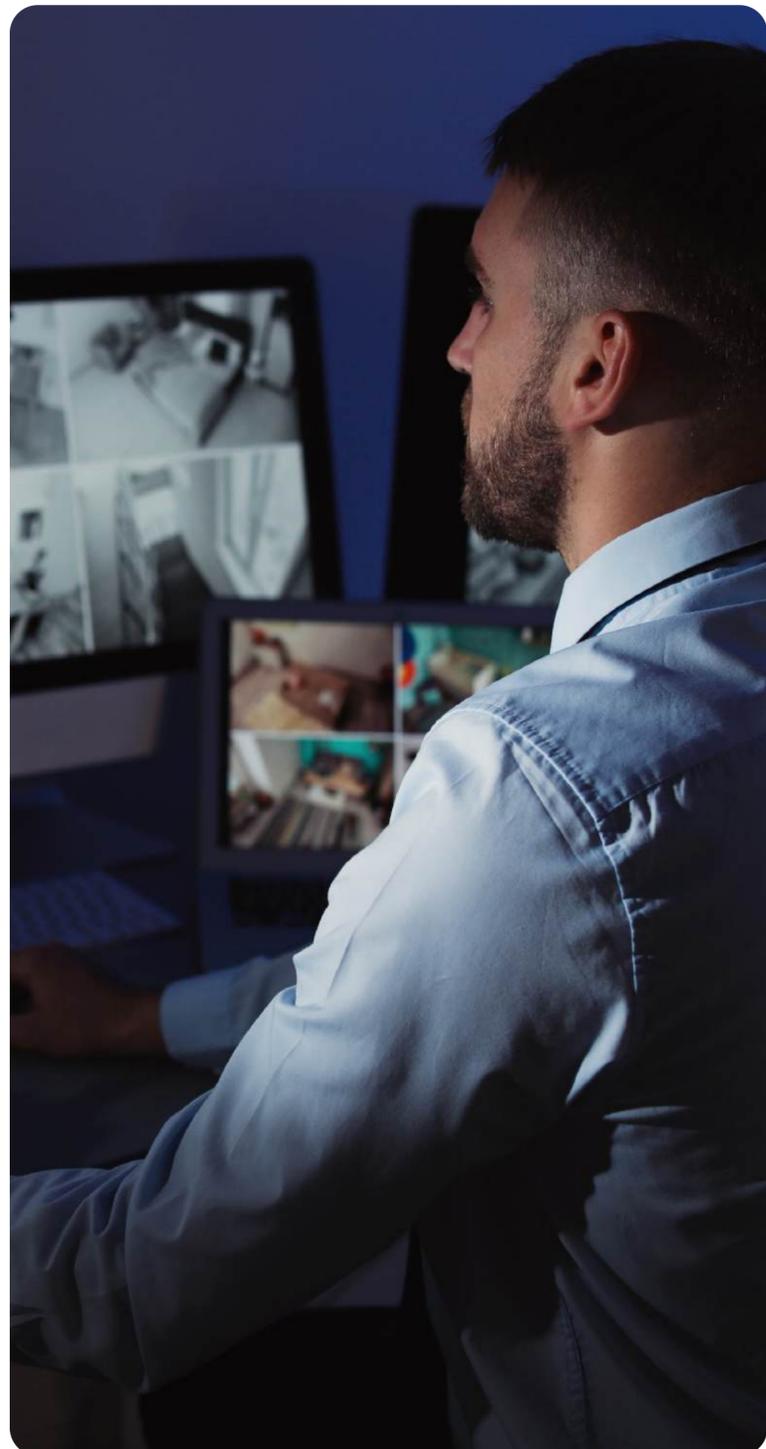
While the need for response is clear, managing it internally creates a fragmented, manual burden.

Many centres mistakenly treat response as a side-task rather than core **response infrastructure**.

“It was almost a blind transfer. You pass the information on and hope for the best. You’re not sure where it lands, you’re not sure when they’ll be there, and you’re not sure what happens next.”

– Rob Dovey, Managing Director at DSOC

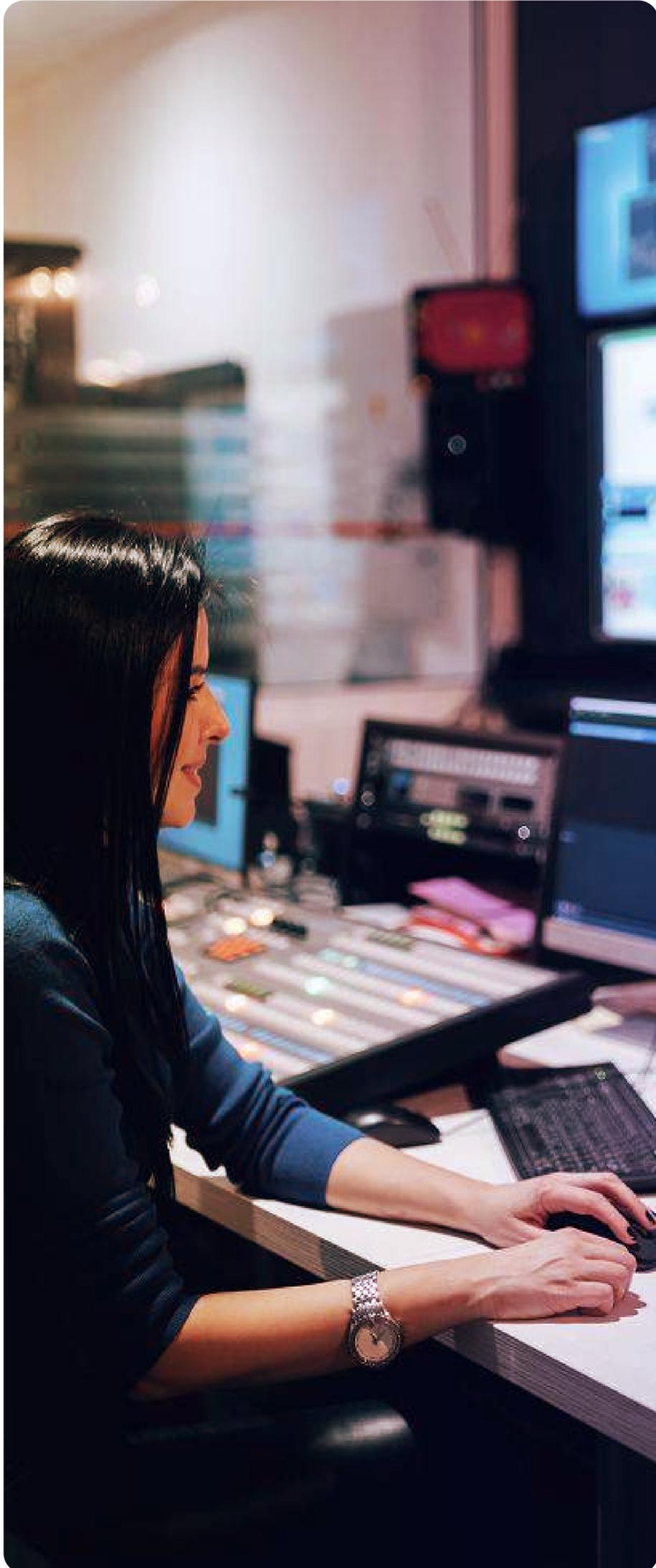
Managing this internally means drowning in administrative overhead: validating **SIA licensing**, checking insurance across different counties, vetting procedures and chasing performance data.



During live incidents, operators are forced into “dispatch trees” – wasting critical seconds calling through phone lists and guessing at ETAs. The true cost of response is not the dispatch fee; it is the accumulated friction of **manual coordination** that drains operator capacity.

The three strategic paths

ARCs face three realistic directions:



Legacy models and public resources

Some organisations rely on national response networks, but these legacy models are often slow and provide limited visibility or quality reporting. As a result, many businesses still fall back on police response or informal keyholders—each with its own limitations.



Internal orchestration

Coordinating your own network of local guard providers allows you to cherry-pick strong regional responders, but it creates administrative overhead. As coverage expands geographically, this model can become increasingly complex, shifting leadership focus from monitoring performance to managing a fragmented field ecosystem.



Plug into scalable response infrastructure

Partnering with a **vettted response network** allows you to convert a fixed infrastructure problem into a scalable, variable-cost solution.

Orchestration: The missing layer

A plug-in security response layer, like AURA, does not replace your monitoring platform; it acts as the coordination layer between verification and physical attendance.

Instead of manual phone calls, activations are matched to the **nearest vetted response network partner** based on **live tracking**. Guesswork is replaced by real-time visibility, and anecdotal evidence is replaced by time-stamped digital proof of attendance.

“What we get now is confirmed attendance, confirmed time scale, confirmed outcome. Digital evidence. The loop is closed.”

– Rob Dovey, Managing Director at DSOC

For operators: this removes repetitive call handling.

For leadership: it provides total visibility into response times and service consistency across the UK, and for clients, it provides reassurance



The commercial impact of infrastructure

When response is treated as infrastructure, your sales conversation changes. Teams can confidently position “monitoring and response” as a bundled offering.

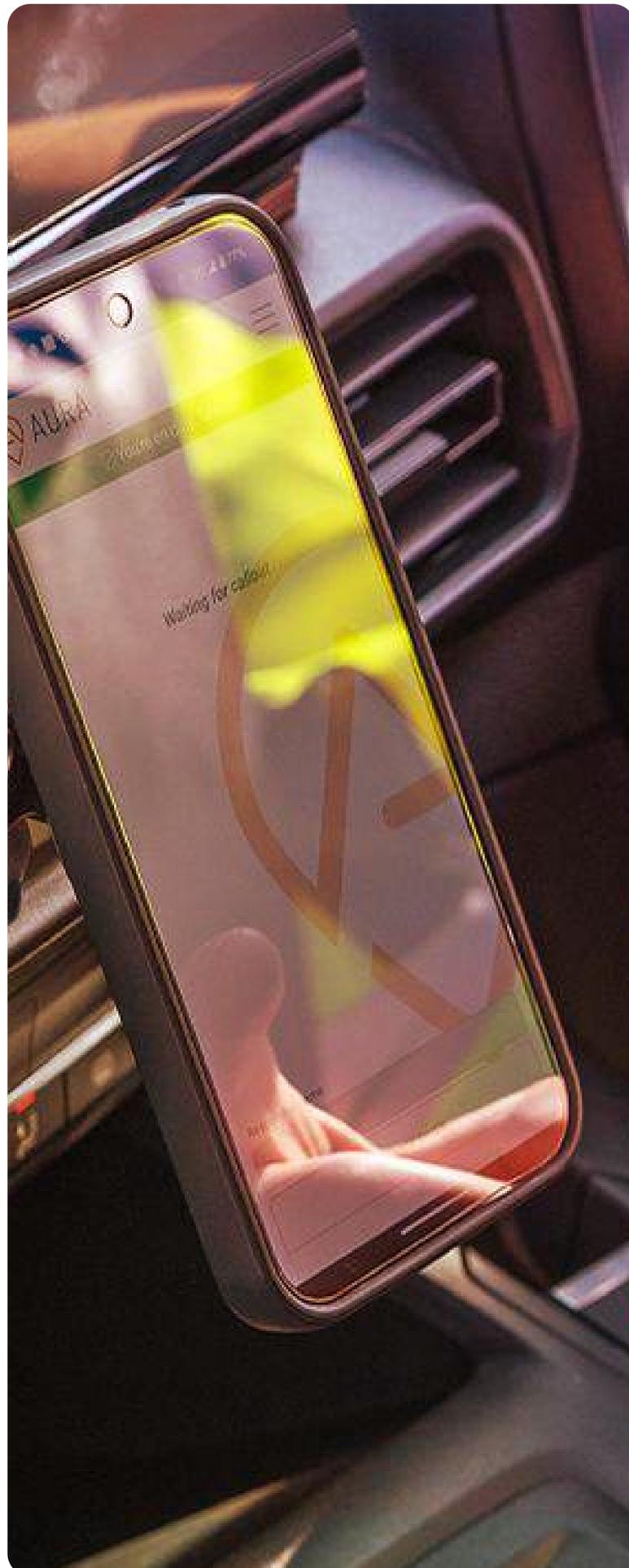
Retention improves because customers experience consistent outcomes. Expansion opportunities emerge as you can package response as a premium tier for multi-site commercial portfolios.

Rob reflects on the contrast with previous arrangements:

“Within three months, an AURA guard detained someone on site. That was the first positive outcome that our customer had seen.”

— Rob Dovey, Managing Director at DSOC

You gain the power of a national guard fleet without the capital burden of building one.



Case Study: DSOC, UK

DSOC (Doncaster Security Operations Centre) uses the AURA network to provide nationwide security response for their rapidly growing customer base.

By integrating AURA's rapid response services directly into their **Sentinel CMS Software**, DSOC enabled dispatches to be created for a site within seconds. The results were transformative:



74%

reduction in
controller time saved
per callout.



24-min

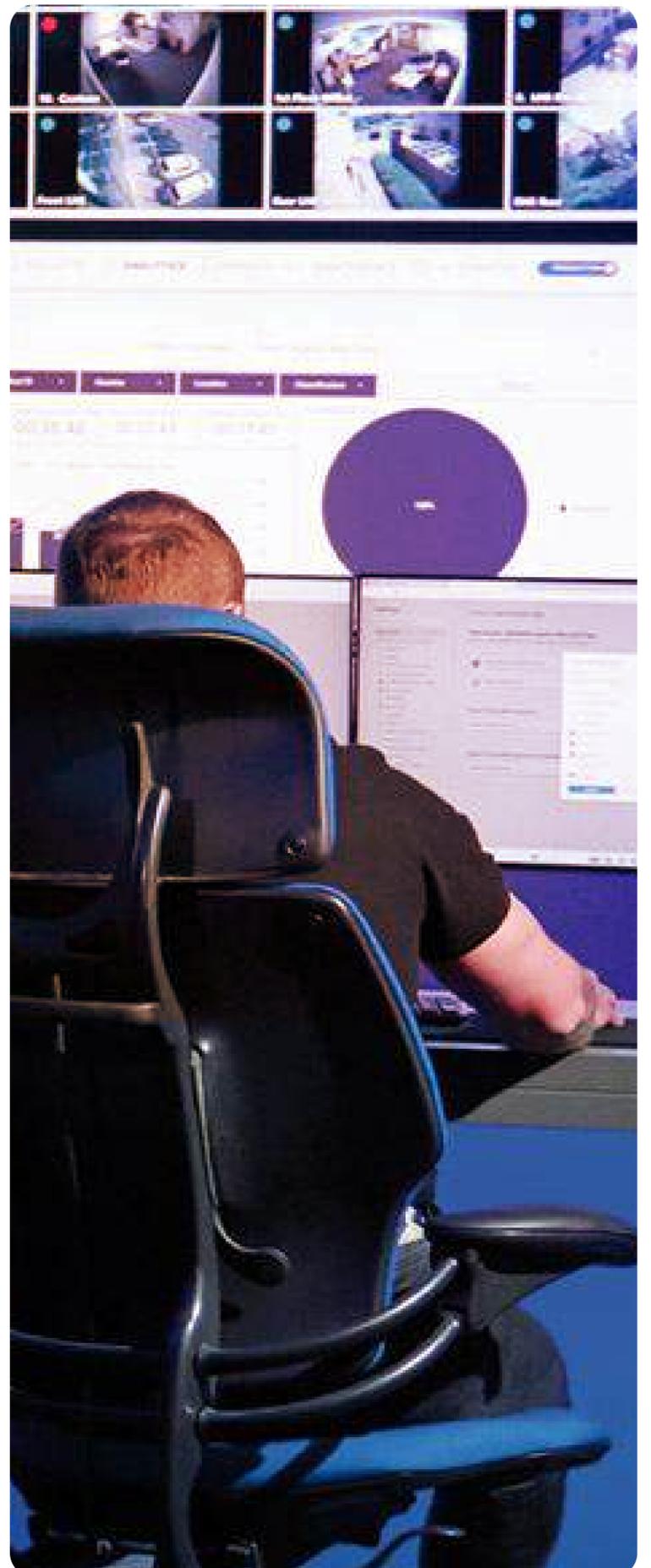
average response
time across their
network in 2024.



Significant operational efficiencies and improved
visibility of activities.

"AURA consistently delivers, with significantly faster response times than other large networks we've used."

– Rob Dovey, Managing Director at DSOC



Protecting your core competency

ARCs excel at monitoring, verification and customer communication. Building a distributed guard workforce requires a different operational discipline.

Plugging into response infrastructure allows you to extend your reach without diluting your focus.

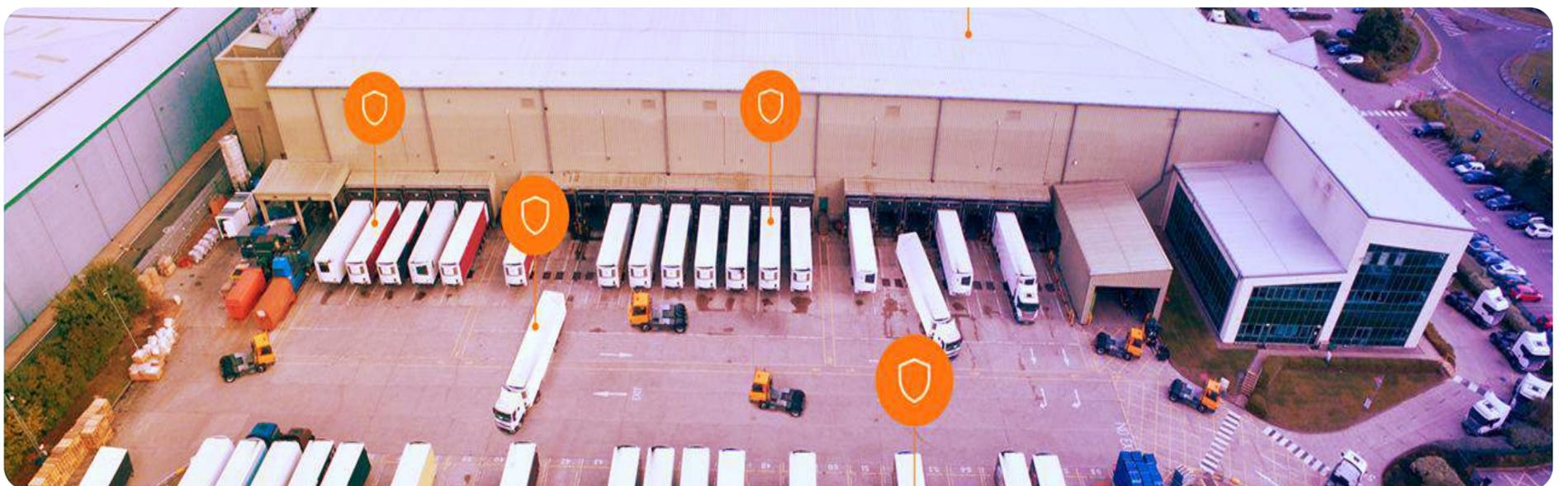
Rob highlights the level of trust now placed in monitoring and response partners:

“They trust us - and by proxy, AURA - to manage the whole workflow.”

– Rob Dovey, Managing Director at DSOC



Modern response infrastructure does not require “ripping and replacing” current systems. Integration occurs via API or structured workflows within your **central management system**. Operators verify incidents as they always have, while the platform handles the heavy lifting of dispatch and reporting.



The infrastructure decision

The UK monitoring industry has evolved from alarm handling to video verification and is now firmly entering the phase of **outcome assurance**.

Clients measure performance not by how quickly signals are processed but by how effectively incidents are resolved.

ARCs that can demonstrate speed, transparency and closed-loop accountability will lead the market. Plugging into national response infrastructure is not about adding complexity; it is about aligning the monitoring model with modern expectations.

AURA also provides access to a nationwide network capable of supporting not only alarm response, but also scheduled patrols, lock and unlock services, static guarding, keyholding and other on-demand security requirements.

This gives ARCs a simple way to strengthen their core alarm offering while also creating new services they can deliver to their customers through a single, connected platform.

The buyer takeaway

Professional monitoring today means managing incidents end-to-end. The ARC that controls the outcome controls the standard.

Reviewing your response model?

AURA supports over 175,000 sites across multiple sectors and already partners with more than 20 ARCs in the UK. Speak to one of AURA's experts about how a plug-in guard response layer can integrate into your existing workflow.

[Book a demo](#)