

The Autonomous Security Playbook

How modern security teams are enabling 24/7 protection with drones that never sleep.

Table of Contents

1. The Shift from Reactive to Autonomous Security

2. The Modern Aerial Security Lifecycle

3. Introducing S.E.C.U.R.E Stack

- S — Sensor Integration
- E — Enterprise VMS Integration
- C — Continuous Monitoring
- U — Unified Command & Communication
- R — Real-Time Intelligence
- E — Emergency Response & Reporting

4. Building Your Autonomous Operations

5. Quick-Win Workflows

6. Data Sovereignty & Compliance

7. The Future of Security Autonomy

The Shift from Reactive to Autonomous Security

Security operations today rely on a strong combination of guards, CCTV cameras, perimeter sensors, scheduled patrols, and quick response teams. These tools and processes work together to maintain full security cover across a site and ensure teams can react quickly when something happens.

What limits these systems is not their capability, but their perspective. Most ground-based tools allow teams to observe what is happening, yet orientation, decision-making, and action often depend on partial visibility. This slows the OODA loop, where every second matters.

Aerial security using drones closes that gap. Drones widen what teams can see, give elevated vantage points, and deliver verified information within seconds. This helps the OODA loop complete faster, allowing teams to respond with clarity and speed while still relying on the systems they already have.

This is not about replacing existing tools. When ground infrastructure is augmented with aerial autonomy, blind spots shrink, response times improve, and security shifts from reactive to proactive.

This playbook brings these learnings together to help security leaders tighten their OODA loop and build security systems that are always-on, adaptive, and autonomous.



The Modern Security Lifecycle

The OODA loop (Observe, Orient, Decide, Act) defines how fast teams can sense and react to threats. Like mentioned before, aerial autonomy amplifies this process by expanding what teams can see, interpret, and act on in real time.

Every alert can be verified within seconds, reducing unnecessary ground deployments and ensuring that resources are used only where they are needed most.

The five phases of autonomous security

1. Detection

Sensors, radars, and AI video analytics continuously monitor perimeters to identify motion, intrusion, or environmental anomalies in real time.

2. Verification

Autonomous drones launch automatically to verify alerts with live visual and thermal feeds, confirming actual events within seconds of detection.

3. Response

Ground teams coordinate with aerial intelligence and live analytics to assess threats, guide response units, and ensure rapid on-site action.

4. Investigation

Every incident is automatically logged with flight data, visual evidence, and mapped event trails for post-incident review and root-cause analysis.

5. Audit

All missions, recordings, and operator actions are time-stamped, archived, and retrievable for compliance validation and operational performance tracking.

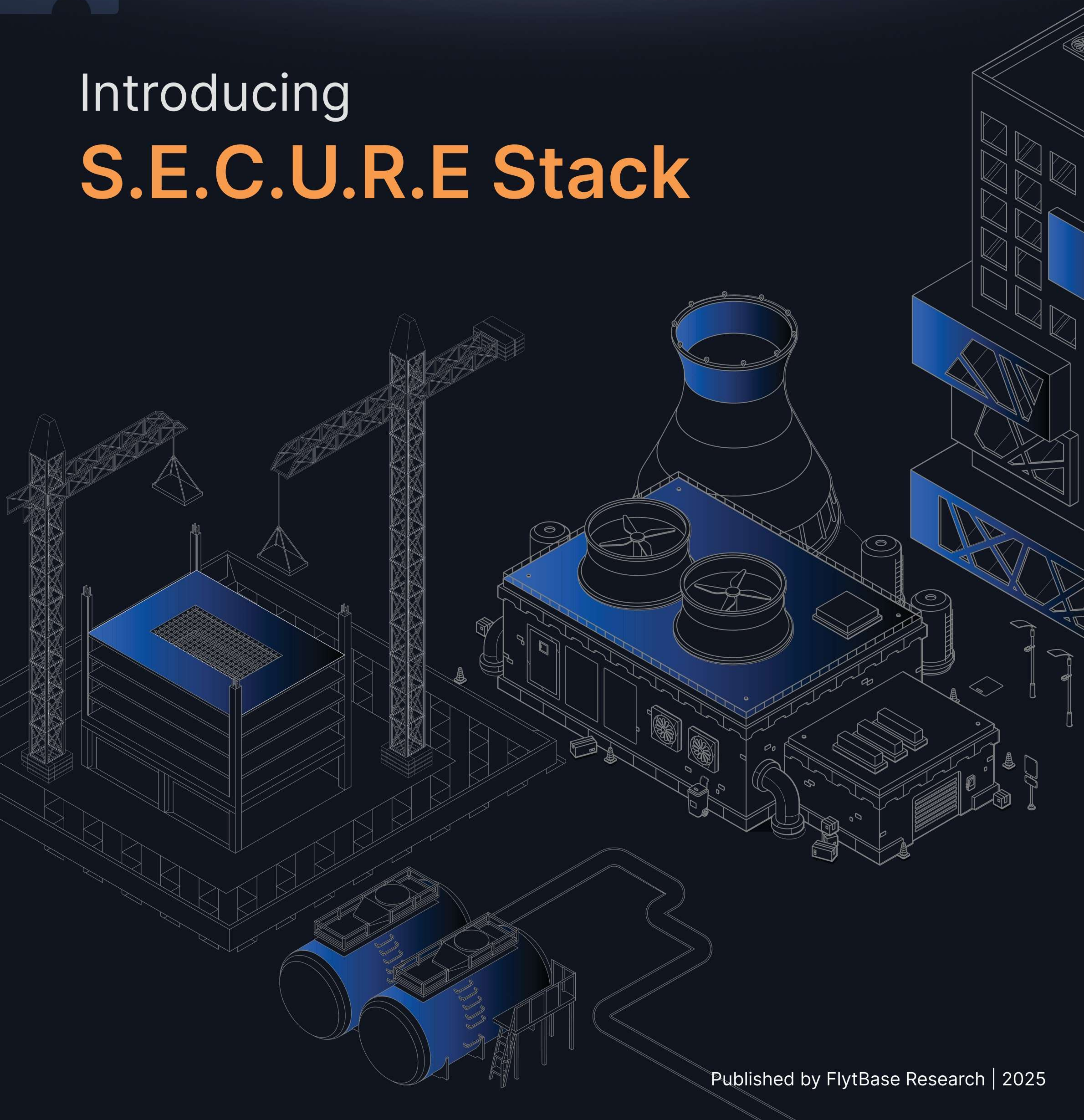


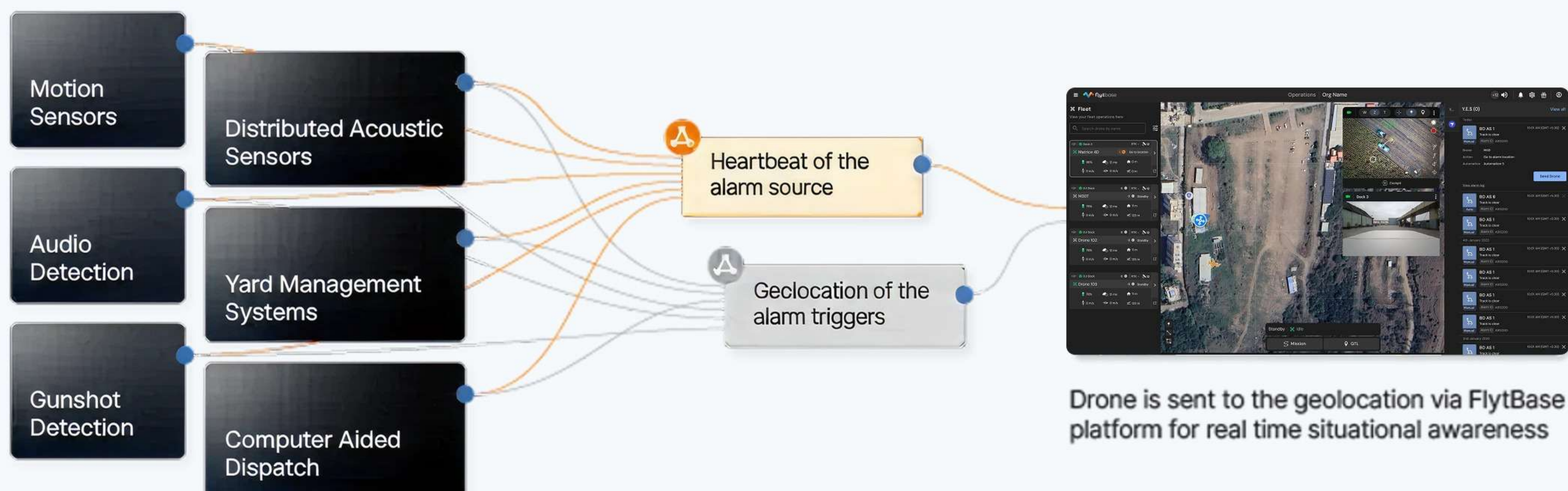
From Detection to Decision: All in One Stack

Every aerial security autonomous operation that FlytBase supports is built on the same foundational elements.

We call this the S.E.C.U.R.E. Stack: six components that together form a complete security ecosystem.

Introducing **S.E.C.U.R.E Stack**





S - Sensor Integration: Turning Alerts into Actions

The Challenge

Most security systems detect, few coordinate. Alarms triggered by motion, heat, or intrusion often remain isolated within their native dashboards, disconnected from the rest of the operation. As a result, alerts either go unanswered or trigger costly manual dispatches for non-critical events.

The Solution

Connect every sensor to an autonomous response network. Each alarm can be mapped to a specific drone and flight path, ensuring the right asset is launched to the right location within seconds. Verified alarms receive immediate aerial confirmation, while false triggers are filtered out without deploying ground teams, saving both time and resources.

The Workflow

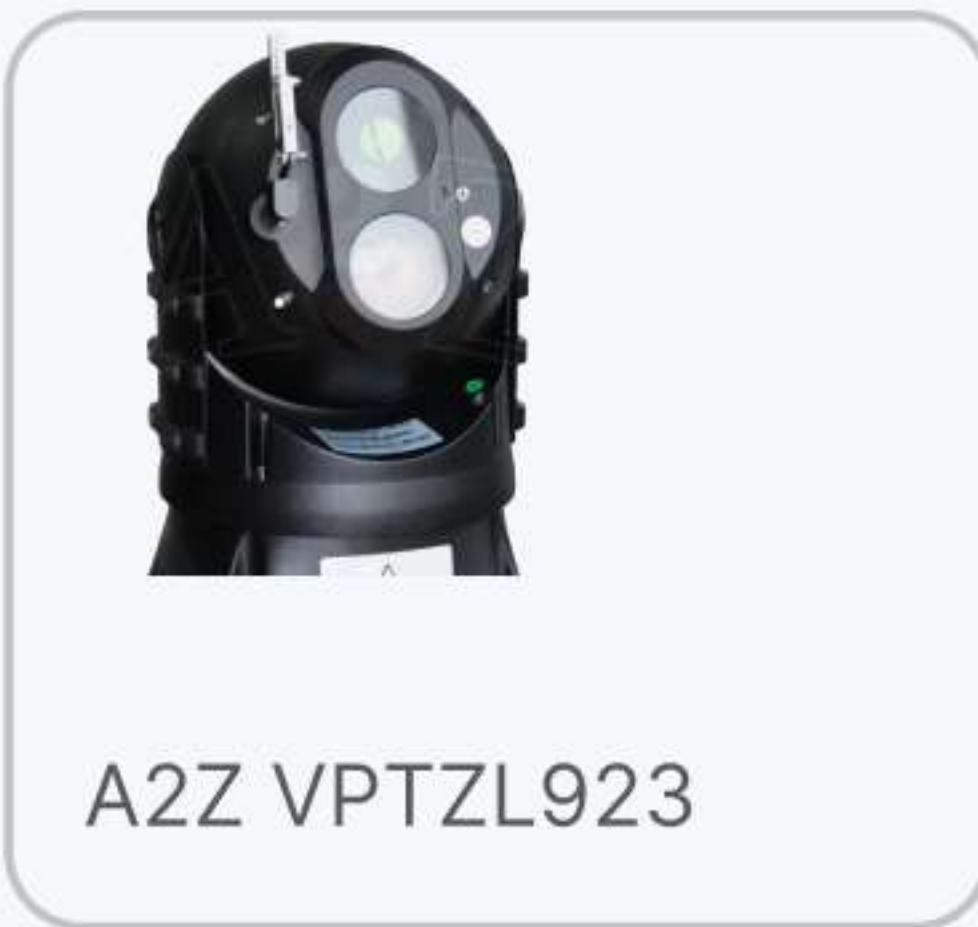
- Integrate any existing alarm, radar, or perimeter system via open APIs.
- Map each sensor to a predefined response zone or mission path.
- Apply multi-sensor logic to prioritize and trigger drone launches only for verified events.
- Stream live video and thermal feeds directly to the command center for instant decision-making.

How FlytBase Can Be Used

FlytBase automation bridges sensors, drones, and command systems into one connected security stack, enabling real-time mapping of alarm events, autonomous verification flights, and intelligent prioritization of true threats.

Supported Security Hardware

- CCTV
- Motion Sensor
- Gunshot Detectors
- DAS
- Fire & Smoke Detectors
- Fence Detector



E - Enterprise VMS Integration: One Unified Command Center

The Challenge

Drone video streams often exist in isolation. While CCTV and alarm feeds flow into enterprise-grade VMS platforms, drone footage is usually managed separately. This disconnect breaks situational awareness and limits how effectively aerial intelligence supports ground operations.

The Solution

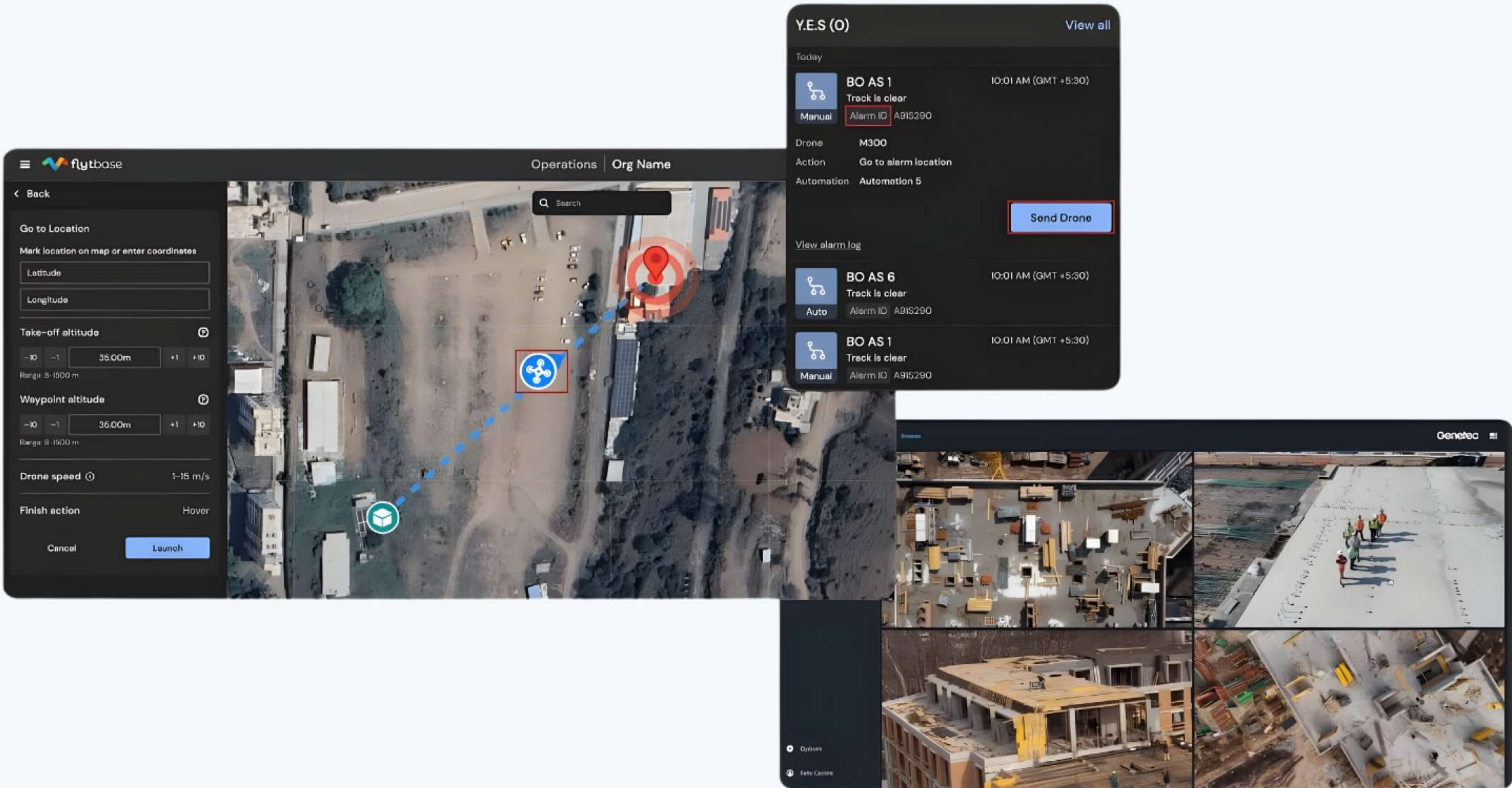
Enable drones to stream directly into existing video management systems such as Milestone, Genetec, or custom PSIM platforms. This creates a unified visual layer where every aerial feed is centrally visible, searchable, and archived alongside fixed camera footage. Operators can view, verify, and act without switching systems.

The Workflow

- Connect live drone streams to your enterprise VMS through FlytBase APIs.
- Sync alarm and mission metadata, including time, location, and trigger type.
- Enable automatic video tagging and archiving for each event or incident.

How FlytBase Can Be Used

FlytBase provides the bridge between autonomous drones and enterprise-grade video management systems, ensuring that aerial data is captured, distributed, and stored as part of the organization’s central security infrastructure.



C - Continuous Monitoring: Making Visibility Uninterrupted

The Challenge

Manual patrols cover limited ground. Human fatigue, shift changes, and blind zones create coverage gaps during the hours most vulnerable to intrusion or incident.

The Solution

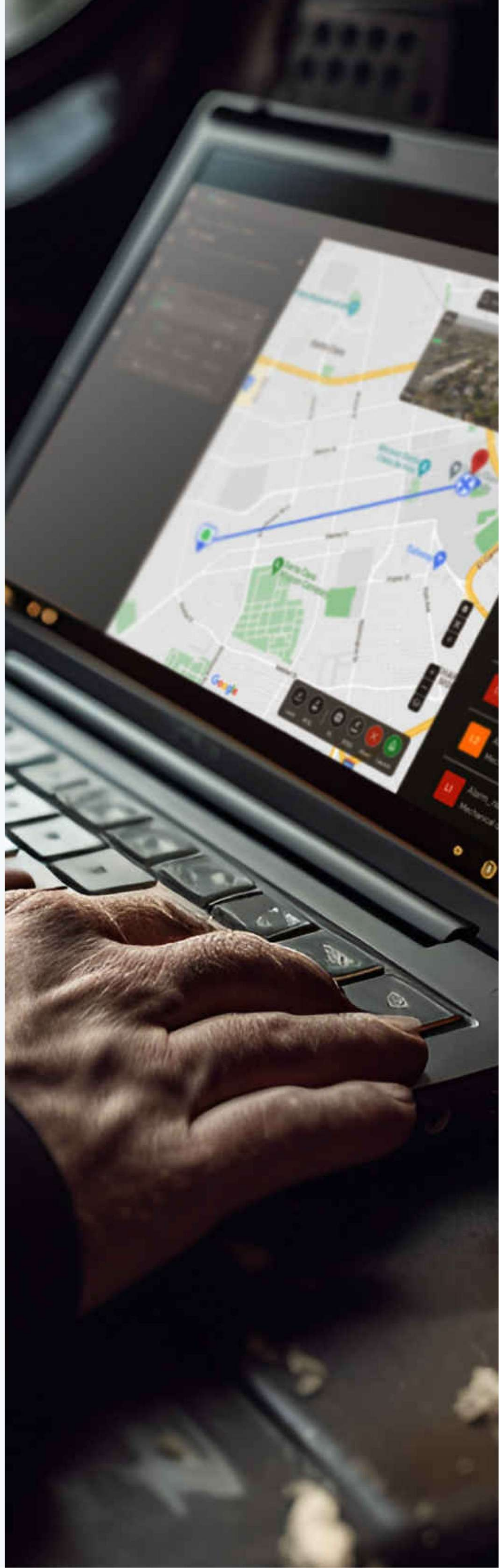
Enable continuous aerial surveillance through scheduled and sequential autonomous missions. As soon as a drone completes charging, it relaunches for the next patrol, maintaining uninterrupted visibility across critical zones without human intervention.

The Approach

- Configure mission frequency per zone based on risk or time of day.
- Enable back-to-back scheduling for continuous patrols during high-risk periods.
- Switch between thermal and visual sensors automatically based on light conditions.
- Archive all flight data and mission logs for compliance and analytics.

How FlytBase Can Be Used

FlytBase's scheduler engine coordinates multi-dock fleets with adaptive battery and weather logic, ensuring that each drone launches as soon as it is mission-ready, achieving true round-the-clock monitoring.



Success Story

Autonomous Drone Surveillance for Plantation Security

Dole Asia, a global leader in fresh produce, manages 24,000 hectares of pineapple plantations in the Philippines. To tackle ongoing challenges such as theft and unauthorized access, Dole partnered with ASY Electronics to deploy DJI Dock 2 drones powered by FlytBase.

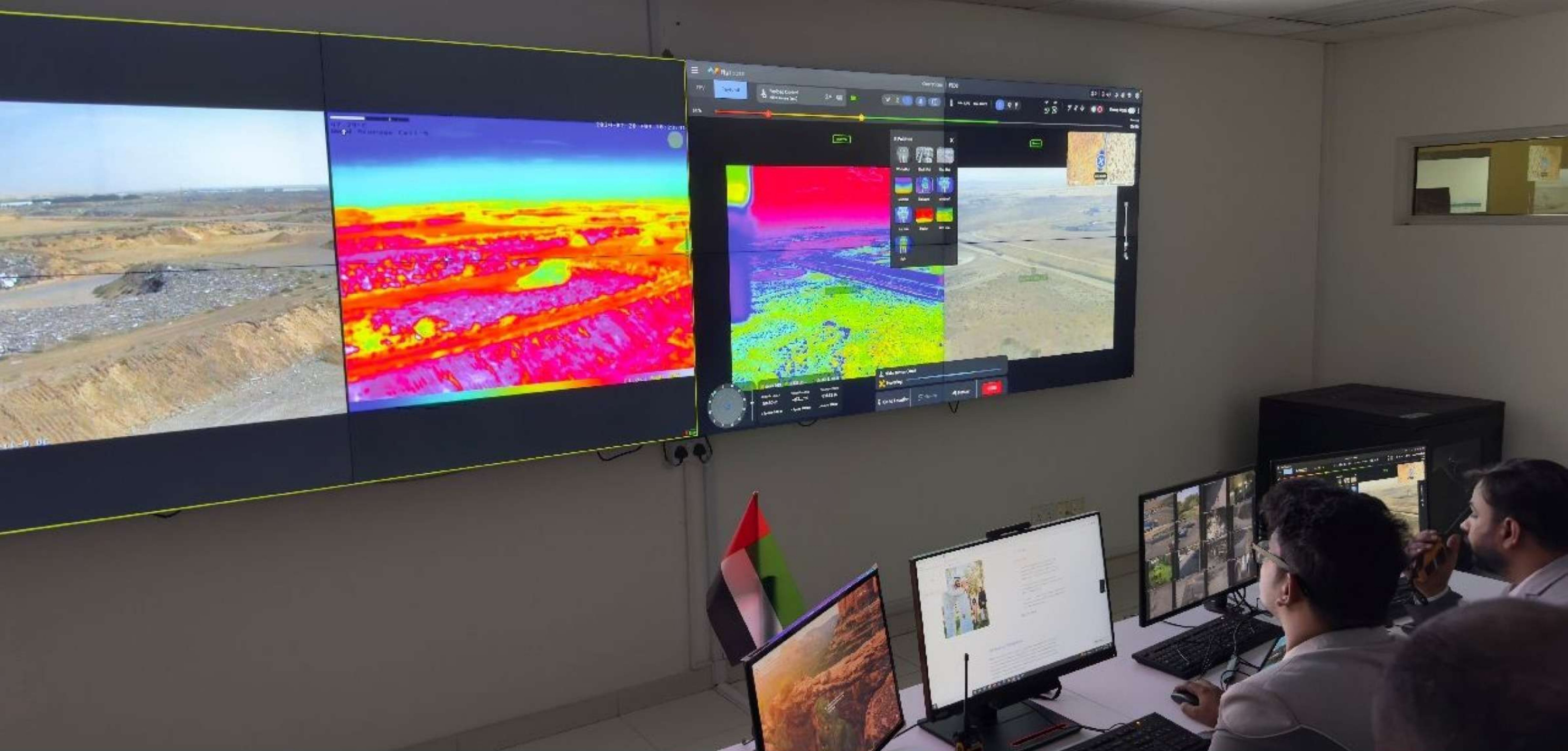
With 24/7 autonomous operations enabled by Drone-in-a-Box (DiaB) systems, the drones deliver real-time aerial surveillance, rapid incident response, and consistent perimeter monitoring. FlytBase's software provided seamless mission automation, centralized control, and live video streaming to Dole's command center—enhancing situational awareness across vast plantation areas. The solution not only improved security but also supported agricultural monitoring by identifying crop anomalies from the air.



"Traditional security in a large geographic environment like this just is not effective. The drones, our control room operating 24 hours a day, our pilots working 24/7, our supervisors out there—all of this coming together has given us a tremendous capability out in the fields."

Tyron Mangakahia, Global Security Director,
Dole Asia Company





U - Unified Command & Communication: Ground + Air + Data

The Challenge

Even the most advanced drones and alarms lose effectiveness when teams operate in isolation. Without a central coordination layer, aerial intelligence never reaches the people responding on the ground. This disconnect delays decisions, duplicates effort, and limits the impact of every mission.

The Solution

Create a shared operational picture for all security personnel. Ground guards, control-room operators, and aerial units stay connected through a common event network. Whether using an enterprise command platform, radio communication, or even WhatsApp, every team member receives live drone feeds and status updates that inform real-time decisions and actions.

The Workflow

- Connect field radios, tablets, or apps to a central coordination channel.
- Stream live drone feeds and mission data to all connected devices.
- Enable guards to relay situational updates or request aerial views instantly.
- Archive communication and mission logs for review and compliance.

How FlytBase Can Be Used

FlytBase integrates aerial operations with ground communication networks. Its event architecture synchronizes data, video, and updates across devices, ensuring that every unit, airborne or on the ground, operates with the same situational intelligence.

Site Security



Premier Security Solutions, a Michigan-based provider operating in 17 states, manages over 4,000 cameras and protects \$4B+ in inventory daily. To enhance protection at high-risk sites, they teamed up with UVT to deploy FlytBase-powered autonomous drones. Integrated with their GSOC, the system enables real-time monitoring, rapid threat detection, and proactive aerial response.

"We've done more than 6,000 flights to date in partnership with UVT, protecting our customer assets and had great success at doing so. We are not reactionary and we are always preparing to be proactive and stop the potential issue before it becomes a problem."

- Todd Lanning, VP of Commercial Operations, Premier Security



Titan Protection, a Kansas City-based security firm, has transformed its operations by integrating autonomous drone technology. This innovation led to a 40% decrease in security incidents and a 60% reduction in costs compared to traditional security methods.

"These autonomous systems allow us to detect and respond to incidents much more efficiently than traditional security officers patrolling on foot, and at a fraction of the cost."

- Ryan Smith, Founder and President, Titan Protection



MSS Security, Australia's largest security provider, has enhanced Port Lincoln Airport's safety by deploying FlytBase-powered autonomous drones. MSS Security conducts regular night time perimeter inspections, effectively detecting security threats, wildlife intrusions, and fence breaches. This integration of AI-powered threat detection with reliable drone control software has improved security coverage and operational efficiency.

"We run this now most nights around the perimeter of the entire airport. It's a much safer, time-effective use of a resource that we can do to find people with ill intent to interfere with aviation."

- Gregory Neyland, Head of Aviation and Emerging Technologies, MSS Security

R- Real-Time Intelligence: From Seeing to Knowing

The Challenge

Even when detection is quick, orientation is slow. It takes time to verify what triggered an alert, identify who or what is involved, and understand how the situation is changing. This delay keeps teams stuck in a reactive cycle instead of moving toward proactive decisions.

The Solution

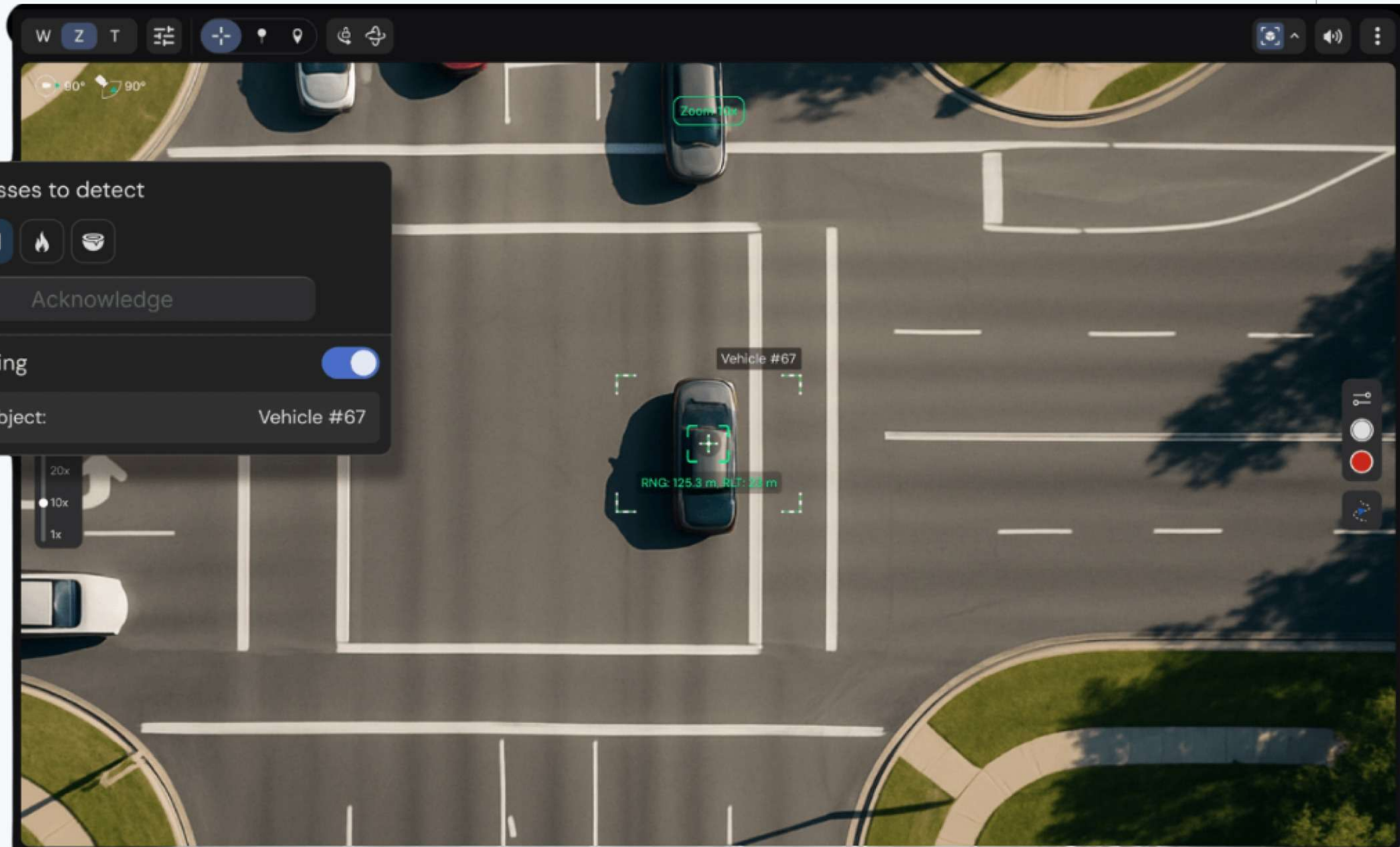
Real-time intelligence streams live visual or thermal data from drones straight to those making the call. Because aerial platforms can change height, angle, and zoom, they deliver both the broad view and the close-up detail of an unfolding event. Coupled with AI detection and tracking, teams can recognize people, vehicles, or anomalies in motion and act while the incident is still developing.

The Workflow

- Stream live drone feeds to the control room or mobile devices.
- Adjust camera angles and flight paths dynamically for optimal visibility.
- Use AI models to detect, classify, and track activity in real time.
- Archive every feed and decision for review and compliance.

How FlytBase Can Be Used

FlytBase enables continuous video and thermal streaming across multiple user interfaces, allowing operators to observe, analyze, and act in real time. Integrated AI modules tag events and track movement directly within the feed, transforming every mission into a live intelligence operation.



E - Emergency Response & Reporting: Closing the Loop

The Challenge

Emergency responses often lack coordinated visibility. Static cameras and sensors provide limited context, while delayed reporting and manual documentation slow down decision-making and investigations. In critical moments, poor communication or unverified visuals can aggravate the situation instead of resolving it.

The Solution

Aerial platforms give responders real-time intelligence without interfering with ground operations. Drones provide flexible perspectives, monitoring from multiple angles, tracking incident progression, and relaying visuals instantly to command centers and emergency teams. Once the situation stabilizes, every image, video, and telemetry log becomes part of a complete digital record, ready for review, investigation, or compliance reporting.

The Workflow

- Stream live drone video to emergency response units and the command center.
- During flight, automatically tag mission data with event IDs and timestamps.
- On landing, upload video, imagery, and telemetry to the evidence management system.
- Verify successful uploads and generate an incident record linked to the mission log.

How FlytBase Can Be Used

FlytBase automates the full evidence chain by connecting aerial data to existing VMS and case management systems. Using webhooks and APIs, you can upload flight data, verify file integrity, and link every mission to its corresponding incident record; ensuring that every response becomes a complete, auditable digital case file.

←

Perimeter Breach Investigation

Report ID: RPT-2024-001 • January 20, 2024 at 2:30 PM

Share

Download PDF

Generated
January 20, 2024 at 2:30 PM

Location
DFL SouthMin - Sector 203A-91

Author
Security Team Alpha

Threat Level
High Risk

Executive Summary

On January 20, 2024, at approximately 14:30, security personnel detected a breach in the perimeter fence at sector 203A-91. Two individuals were observed removing a section of the fence using cutting tools. Immediate response was initiated, and the breach was secured within 45 minutes. No equipment or materials were reported missing from the facility.

Incident Details

Nature of Incident:
Unauthorized perimeter breach with fence cutting equipment

Individuals Involved:
Two unidentified individuals, approximately 25-35 years old, wearing dark clothing

Equipment Used:
Wire cutters, bolt cutters, and what appeared to be surveillance equipment

Detailed Observations


Person

Priority: Medium

Intruder Detected

Status: Pending

Please review this image



[Download Original](#)
[Download Annotated](#)

Success Story

Emergency Response via Drone Docks

OvrWatch, a leader in emergency response solutions, collaborated with the Asheville Police Department to enhance disaster recovery efforts following Hurricane Helene's impact on Asheville, North Carolina. The hurricane caused widespread flooding, necessitating rapid and efficient damage assessments across the city.

To address these challenges, OvrWatch deployed a network of 13 autonomous drone docking stations strategically throughout Asheville. This implementation enabled real-time aerial monitoring, expedited damage evaluations, and improved coordination with emergency services. The drones' integration with the city's 911 dispatch system allowed for immediate deployment to critical areas, significantly reducing response times and enhancing situational awareness for first responders.

OVRWATCH

"It's really cool to go in there and just see that anytime there's a call, within a minute or two, they're out on-site with the drone. For them, the thing that makes them the most passionate is just being able to respond anywhere in the city at any time."

Rhys Andersen, Founder and CEO,
OvrWatch





Building Autonomous Aerial Operations

Autonomy isn't a technology milestone; it's a maturity process. Each phase represents a shift in mindset, from manual control to system orchestration. FlytBase models this as a four-phase evolution, achieved by most organizations in 6–12 months depending on scale and regulation.

1 Map and Assess

The goal here is awareness. Before automating anything, teams must visualize their environment and pinpoint where drones add the most value.

Key Activities:

- Map perimeters, entry points, and sensor coverage zones.
- Identify assets that need continuous oversight (fuel depots, gates, storage yards).
- Benchmark current response times.
- Audit existing VMS, alarm panels, and communications systems for integration readiness.

2 Connect & Integrate

Once the environment is mapped, the focus shifts to connecting systems. This phase lays the foundation for autonomous workflows.

Key Activities:

- Integrate sensors and alarms through FlytBase APIs.
- Link VMS or PSIM to receive live drone feeds.
- Establish geofencing and automation logic per site.
- Test alert-to-launch latency (target <15 seconds).

3 Operationalize & Train

This is the turning point, where autonomy meets operations.

Key Activities:

- Run hybrid missions (part scheduled, part alarm-triggered).
- Train control-room staff on drone alert verification.
- Create SOPs for human-in-loop intervention and regulatory compliance.
- Conduct joint drills with ground forces to align air-ground coordination.

4 Scale & Optimize

After operational success at one site, it's time to replicate.

Key Activities:

- Deploy multiple docks across sites and departments.
- Centralize control through a unified ROC.
- Add AI modules for anomaly detection and predictive analytics.
- Standardize mission templates and response protocols

Metrics to track:

- Response Time Reduction
- False Alarm Elimination
- Cost per Square Km Covered
- Operator-to-Drone Ratio

Quick Win Workflows

Every organization can implement a few workflows immediately, no redesign required. These use cases deliver visible results fast, helping teams experience autonomy in action while building internal confidence for larger rollouts.

Alarm-to-Drone Dispatch

When an intrusion alarm triggers, FlytBase launches a nearby docked drone to the coordinates, streams live video, and sends verification to guards.

Benefit: Cut response times to 30 seconds

Scheduled Perimeter Patrols

Set drone patrols every hour with thermal imaging.

Equip with thermal

Benefit: Preventive visibility, reduced human fatigue

visibility, reduced human fatigue

Guard-Requested Support

A guard in the field taps a tablet → drone takes off → provides aerial visibility.

Benefit: Rapid “eyes in the sky” for ground teams

Multi-Site Coordination

Connect multiple docks under one dashboard.

Benefit: Centralized oversight for national or regional operations

Automated Evidence Logging

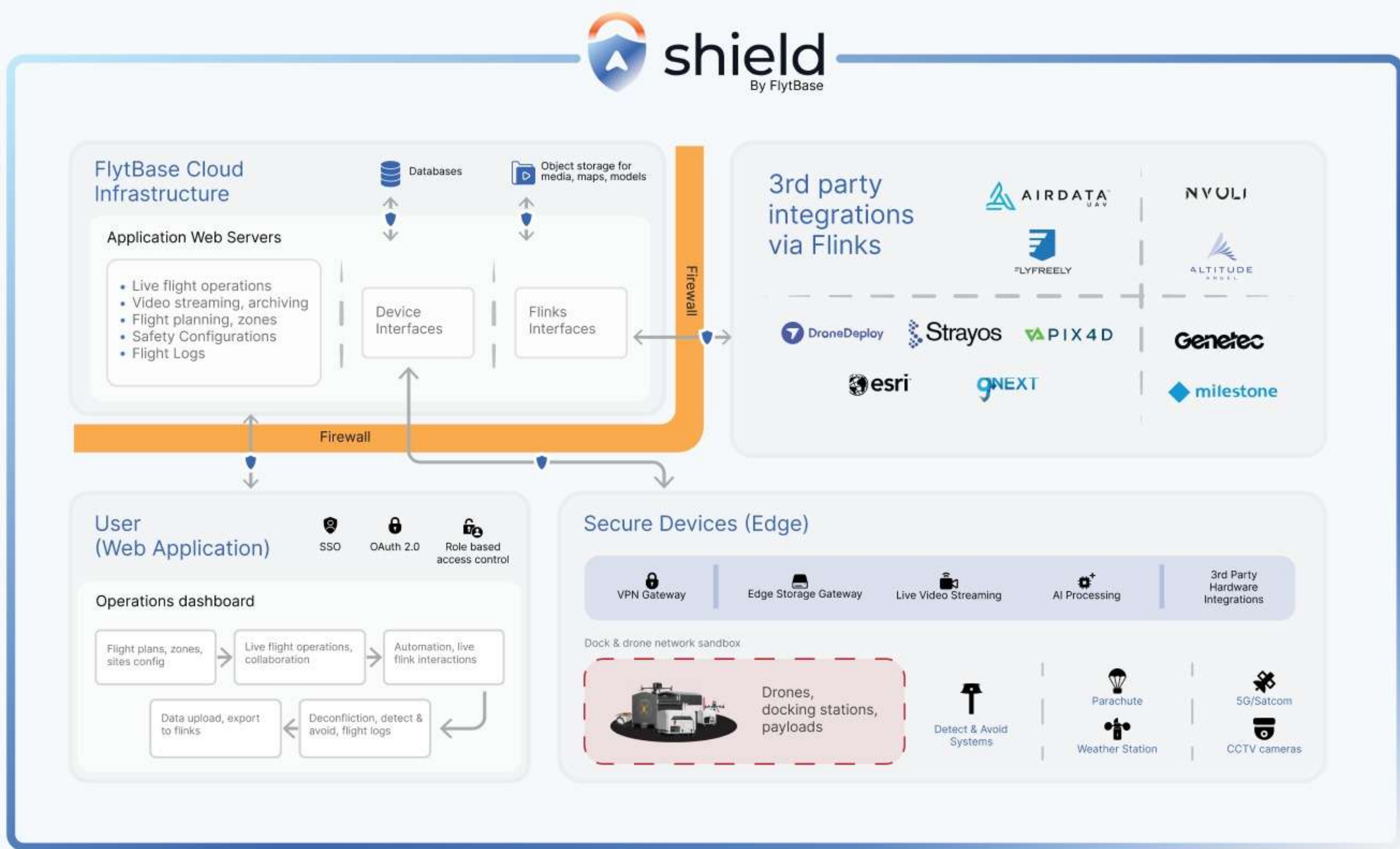
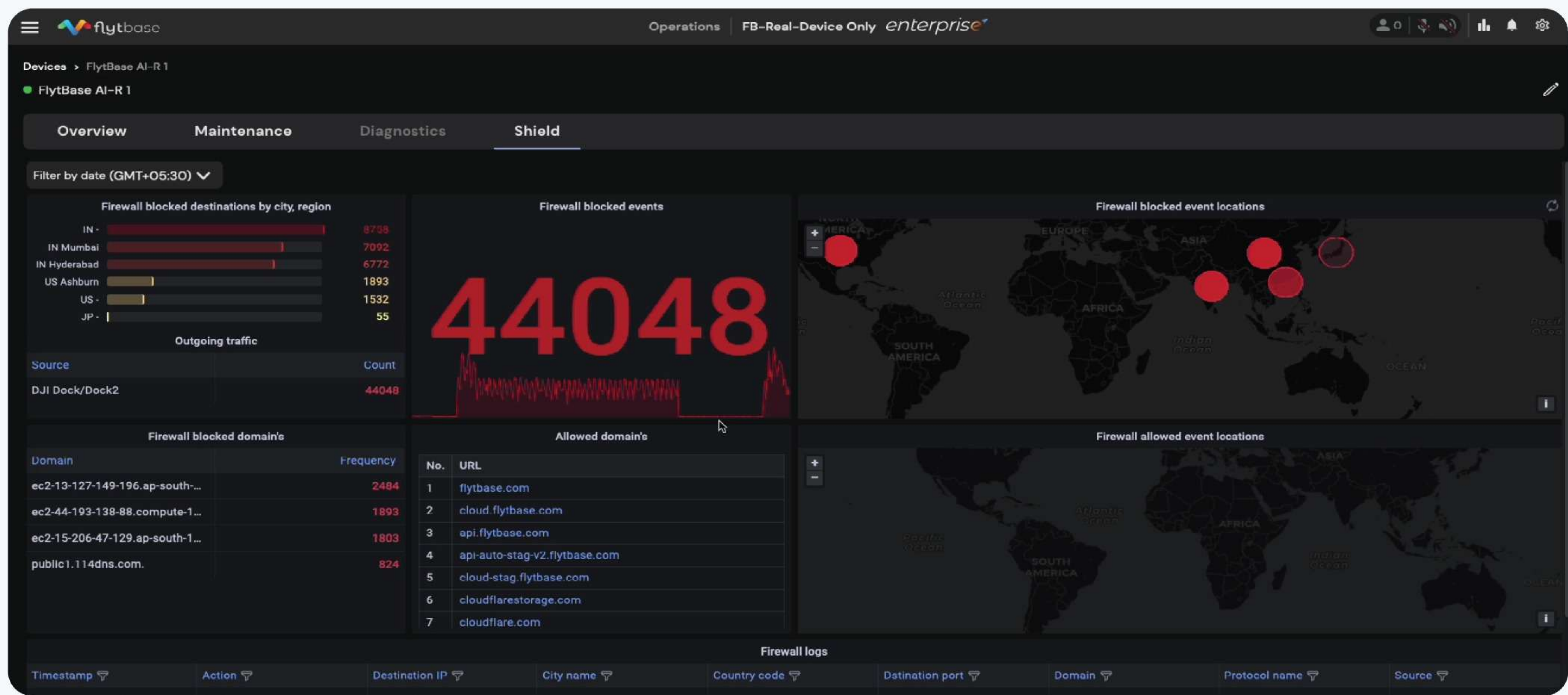
Each flight automatically logs video and telemetry making incident and shift reports.

Benefit: Instant documentation for compliance

“These are the same workflows running live in active operations across five continents today.”
- FlytBase

Data Sovereignty & Compliance

Gain full control of drone data with a secure sandboxed environment. Monitor network activity, enforce firewall protection, set allow/deny lists, track via interactive maps, and automate server blocking by region.



Ensure secure drone operations with end-to-end encryption, AWS-hosted servers, firewalled environment, customizable access controls, and flexible deployment options, including on-premises deployments.

Cloud

A complete firewalled solution, complying with SOC2 Type II, ISO 27001, and GDPR standards, it enables integration with private cloud storage.

Air-Gapped

FlytBase Air-Gapped operates offline, isolated from external networks, ensuring data security. It is ideal for sensitive applications that require maximum protection.

In-country Cloud

A solution to host FlytBase on your own country's cloud to ensure compliance with data residency norms, data security, and the ability for customers to integrate with their preferred applications.

On-premises

Ability to self-host FlytBase on a private server for highly secure and confidential projects. Meet cyber security compliance and requirements and have complete control over your drone data.

The Future of Security Autonomy

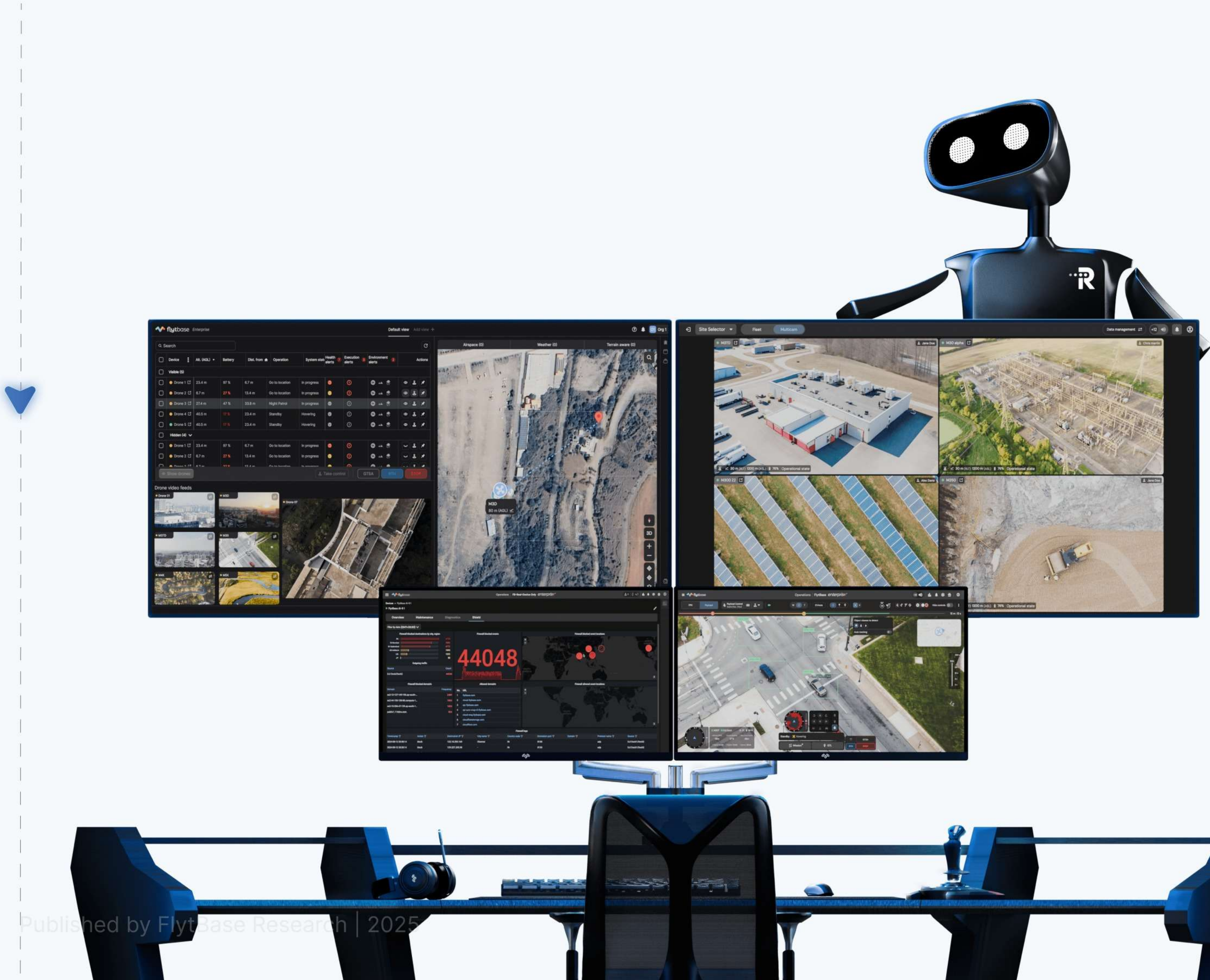
Autonomous security is not about drones; it's about orchestration. Tomorrow's systems will predict threats, coordinate across agencies, and learn from every mission.

As AI models advance and regulatory frameworks mature, the lines between response and prevention will blur, creating security systems that are as proactive as they are protective.

- AI pattern analysis to forecast intrusions.
- Swarm coordination across multiple docks.
- Smart-city integrations linking public and private assets.
- Collaborative autonomy, where air and ground units act as one.

At FlytBase, we see a future where every critical site, from an oil terminal to a temple, has its own autonomous security layer, continuously protecting people and infrastructure.

Because security doesn't stop. And with autonomy, neither should your systems.



Autonomous Security Operations Readiness Checklist

Use this checklist to evaluate whether your security organization is ready for autonomous, continuous operations across facilities, campuses, and infrastructure assets.

Each section represents a capability proven in scaled deployments across enterprise, government, and critical infrastructure security. The more checks you can tick, the closer your operation is to true autonomous readiness, where incidents are detected, verified, and responded to automatically, with full compliance and oversight.

1. Alarm-to-Drone Automation

- ☐ Can your drones auto-launch within 30 seconds of a perimeter breach, motion alarm, or access control trigger?
- ☐ Can flight plans adapt in real time based on the alert location, weather, or no-fly zones?
- ☐ Can a single operator supervise multiple autonomous missions simultaneously?
- ☐ Can missions be triggered directly from alarm panels, PSIM dashboards, or security analytics software?
- ☐ Are response metrics, launch latency, time-to-visual, and verification accuracy, tracked automatically?

2. Continuous Patrol & Visibility

- ☐ Can autonomous patrol missions be scheduled per site, shift, or risk level without manual oversight?
- ☐ Can drones automatically switch between visual and thermal payloads based on lighting conditions?
- ☐ Can perimeter routes be adjusted dynamically for high-risk zones or after incident alerts?
- ☐ Is there automated health monitoring for docks, batteries, and communication links?
- ☐ Are all mission outcomes, video, telemetry, and detection data, stored and retrievable for audit?

3. Real-Time Intelligence & AI Verification

- ☐ Can your AI models distinguish humans, vehicles, and animals from live video feeds?
- ☐ Can thermal analytics detect heat signatures, fires, or hidden intrusions?
- ☐ Can AI detections automatically trigger follow-up missions or guard dispatches?
- ☐ Can the system learn from operator feedback to improve accuracy over time?
- ☐ Are detections logged, validated, and exported in audit-ready formats?

4. Command Center & System Integration

- ☐ Are drone video feeds integrated with your existing VMS, PSIM, or alarm systems (e.g., Genetec, Milestone)?
- ☐ Can operators view and manage all ground and aerial feeds within a single interface?
- ☐ Can alarms from different systems trigger a unified workflow across sites?
- ☐ Can events, logs, and footage write back automatically to your incident management or reporting tools?
- ☐ Is there centralized control for multi-site operations with the option for local overrides?

5. Ground–Air Coordination & Communication

- ☐ Can field guards request drone support directly from tablets or mobile devices?
- ☐ Can control centers relay live drone feeds to ground responders within seconds?
- ☐ Can multiple security agencies or departments collaborate through shared visual access links?
- ☐ Is every mission time-stamped with who triggered it, who monitored it, and what actions followed?
- ☐ Can decentralized teams (without a fixed ROC) coordinate through event-based communication systems like radios or messaging apps?

6. Compliance, Governance & Data Security

- ☐ Are all flights, triggers, and responses logged automatically for audit and investigation?
- ☐ Is video data encrypted in transit and at rest under AES-256 or higher standards?
- ☐ Can mission and incident data be hosted entirely on-premise or within private cloud environments?
- ☐ Are retention, access, and deletion policies aligned with enterprise cybersecurity protocols?
- ☐ Can compliance reports be generated automatically for site audits or insurance documentation?

7. Safety, Reliability & Redundancy

- ☐ Does your system maintain over 99% operational uptime with redundant communication links?
- ☐ Can operations continue autonomously after network interruptions (store-and-forward logic)?
- ☐ Are geofencing, return-to-dock, and fail-safe termination policies active for every drone?
- ☐ Are emergency recovery protocols tested under different weather and site conditions?
- ☐ Are system checks for readiness (battery, connectivity, flight area) conducted automatically before launch?

8. Training & Operational Standardization

- ☐ Are all operators trained on documented SOPs within the autonomy platform itself?
- ☐ Can new users simulate missions or replay incident responses for learning purposes?
- ☐ Are incident templates preloaded for perimeter breach, fire detection, or unauthorized entry?
- ☐ Are operator certifications, permissions, and airspace compliance logs digitally tracked?
- ☐ Are lessons from previous incidents reviewed to improve future automation logic?

9. Scalability & Multi-Site Oversight

- ☐ Can your autonomy platform manage multiple docks and fleets across geographies?
- ☐ Can missions be scheduled and monitored centrally while executed locally?
- ☐ Can regional ROCs share visibility across public safety, operations, and IT teams?
- ☐ Can mixed hardware fleets (different drone models or dock systems) operate under one control system?
- ☐ Are cost savings, reduced manpower, and faster response metrics tracked automatically to measure ROI?

Consult our drone autonomy and AI experts
to get started with your **site operations**

contact@flytbase.com
flytbase.com
+1 408-440-7216