

ENTERPRISE INTEGRATION & SECURITY

Fit your architecture. Support your operation.

AirSentinel is built to contribute sensing and intelligence to the systems an organization already uses. Connect AMS directly to a third-party platform, bring mixed sensors into Atlas, or deliver AMS and fused sensor intelligence from Atlas to another command environment. Define the integration around the information your team needs and the people authorized to use it.

Three integration paths. One operational objective.

The sensor supplier and the operator's command platform do not have to be the same company. AirSentinel supports these deployment patterns:

AMS into your platform

Use local or cloud JSON APIs to bring AMS intelligence into a compatible C2, drone detection, security or intelligence platform. Retain the system your operators already use while adding AirSentinel sensing.

Third-party sensors into Atlas

Bring compatible external RF, radar and optical observations into Atlas alongside AMS. Specify the information each source contributes and how it will support the operational picture.

Atlas into another command system

Deliver AMS intelligence and configured sensor-fusion output to downstream C2 and intelligence platforms. Use Atlas as part of the intelligence architecture while keeping the broader response workflow in another system.

Choose sensing by the job it needs to do.

RF, radar and optics contribute different forms of evidence. RF can provide identifiers and reported location. Radar adds physical tracks. Optical and thermal cameras help personnel examine an object or area of interest. An integration should preserve those distinctions while making their combined information useful.

AirSentinel integrates Echodyne radar and optical systems from manufacturers including Axis and Bosch. The architecture remains vendor agnostic: device selection follows the mission, available interfaces, site conditions and required data. Compatibility and the intended handoff are established for the proposed deployment.

ENTERPRISE INTEGRATION & SECURITY

Data & authorized access.

Define the information that has to arrive.

A successful integration starts with the information the receiving team needs: aircraft position, relevant source identifiers, movement, historical context and available ground-location information. Aircraft position, control-station position and takeoff location represent different things and should remain distinguishable at the destination.

The integration plan defines field mapping, coordinates, timestamps and the expected behavior when an observation becomes stale or a source is unavailable. Test the complete handoff with representative aircraft and the network conditions used in operation. Data acquisition, delivery, alert transport and human response should be measured separately.

Connect the team. Define the access.

Atlas supports access roles and authorized sharing so monitoring staff, site personnel and participating partners can use information appropriate to their responsibilities. The deployment plan should identify who administers the environment, who monitors activity and who receives event information.

Authorized shared-flight views let a recipient open an event in a browser without installing an app or managing a separate login and password for that view. This reduces the steps between receiving an event and reviewing its context. Administrative and wider platform access remain governed by the deployment's permissions.

Platform administration and broad data access are separate from an authorized shared-flight view. Define recipients and information-sharing responsibilities as part of the deployment.

ENTERPRISE INTEGRATION & SECURITY

Deployment readiness.

Bring security requirements into the deployment plan.

AirSentinel documents authenticated integration APIs. Open interfaces describe interoperability, not unrestricted public access. Enterprise and government teams should define required user access, network boundaries, data handling and system-assurance controls at the start of the project.

That review should address the data exchanged with external systems, who is authorized to receive it, the role of shared event views and the responsibilities of each integrated platform. Procurement requirements for security controls, retention, hosting and support should be documented for the selected configuration and contract. Request configuration-specific security documentation during technical review.

Plan the installation and the operational handoff together.

AMS supports Power over Ethernet, LTE cellular connectivity and Ethernet, with cloud and local API access. Match the power, backhaul, mounting and environmental requirements to the specific installation. A local API is an integration option; the intended behavior during connectivity loss must be addressed in the deployment design.

Define site acceptance around the actual mission: representative aircraft, required coverage, simultaneous activity, data freshness, camera or radar handoffs and the path to authorized personnel. Agree who owns monitoring, escalation and ongoing configuration before the system enters service.

Start the technical conversation

Bring your existing platforms, required data, access and network requirements, and site acceptance criteria. AirSentinel will scope compatible interfaces and the operational handoff for the selected deployment.

info@airsentinel.ai | +1 (844) 771-8711