BUILT BY A TEAM THAT HAS SECURED MAJOR AEROSPACE INSTITUTIONS WORLDWIDE FOR 25 YEARS.

ARGENT FOR AEROSPACE

AI AGENTS NOW ACT LIKE STAFF. PUT A CHECKPOINT IN FRONT OF EVERY ONE.

Argent Strategic Intelligence puts a checkpoint between your AI agents and the AI services they use. It checks each request first and runs inside your walls. Giving a foreign person controlled technical data can count as an export, even in the US,[1] and two aerospace and defense contractors settled cybersecurity claims for $13 million.[2]

One pane of glass for your entire agent ecosystem: every agent, model, tool, owner and dollar in one view. **No rip and replace.** Argent works with what you already run: your identity provider (Okta, Microsoft Entra, LDAP), your own secrets vault (HashiCorp Vault, AWS Secrets Manager, CyberArk Conjur) and the AI tools your staff already use.



SEE.
Every agent, its owner, where it sends data.



PROVE.
A signed record of every decision.



STOP.
Unapproved models, tools and leaks are refused.

THE FIVE THINGS AEROSPACE FIRMS ASK FOR FIRST

1	**Budget controls** A test-data agent runs up a large bill over a weekend.	Set spend caps by team, person and agent. An agent that hits its cap is stopped; its owner asks for more, and nothing is granted until a manager approves, in Argent or through your ServiceNow or Jira tickets. Project cost tracking shows what each project or program spends on AI.
2	**Data protection** An engineer pastes an export-controlled table into an AI.	Argent reads each request and catches your own export-control markings, part-number formats and lists, and excerpts of registered documents before anything leaves. A match is blanked out or refused; the record names the kind, never the data.
3	**Auditing for auditors** An auditor asks which AI tools touch controlled data.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. A customer's auditor or internal audit can check a package of it on their own computer and see whether anything was altered.
4	**Model control** A team points its assistant at whichever model is cheapest.	Only models you approve are allowed, including one on your own servers; all else is refused. Group them into model classes, such as approved for controlled data. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Controlled technical data must never leave the building.	Argent runs entirely inside your own walls, even on a fully air-gapped network. The install bundle is checked at every step as it crosses into your closed environment.

WHAT REGULATORS ALREADY EXPECT

ITAR, 22 CFR 120.50 and 127.10. Releasing technical data to a foreign person in the US is a deemed export.[1] Each violation: up to $1,271,078 or twice the deal's value.[3]

Defense contracts, DFARS 252.204-7012. Report a cyber incident within **72** hours of discovery, and pass the clause to subcontractors handling covered defense information.[4]

HOW AN AEROSPACE FIRM STARTS

1. Watch mode. A real-time audit and view of what your AI is doing today. Nothing is blocked.

2. Enforce mode. Switch on blocking one area at a time: controlled data, budgets, models, then tools.

3. Inside your walls. Runs on your own hardware or in your own cloud VPC. Nothing leaves the perimeter without your explicit approval.

BOOK A DEMO. WE WILL SHOW YOU ARGENT WORKING ON YOUR OWN AEROSPACE USE CASES.

NYEDIS.AI/DEMO

Sources. 1 22 CFR 120.50(a)(2), ITAR, eCFR, read 2026-11-13. 2 US Department of Justice, release on a $13M contractor cybersecurity settlement, Nov 3, 2026. 3 22 CFR 127.10(a)(1)(i), ITAR, eCFR (90 FR 1868, Jan 10, 2025). 4 DFARS 252.204-7012, acquisition.gov, read 2026-11-13.