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

ARGENT FOR TRANSPORTATION

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 outside AI services they use. It checks every request before it leaves, and it runs entirely inside your own company. A data breach at airlines, railroads, trucking and delivery companies now averages **$4.50** million, up from **$3.98** million.[1]

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 CARRIERS ASK FOR FIRST

1	**Budget controls** A rebooking agent loops all night and the AI bill triples.	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 business unit spends on AI.
2	**Data protection** A notice agent sends passport and card numbers to an AI.	Argent reads each request and blanks out US passport, card, phone and driver's license numbers before anything leaves (names where switched on, booking-reference patterns you add). The record notes the kind of data, never the data.
3	**Auditing for auditors** A regulator asks which rebooking agent sent what, and when.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. An outside auditor or internal audit can check a package of it on their own computer and see whether anything was altered.
4	**Model control** Dispatchers start using an AI model nobody approved.	Only models you approve are allowed; everything else is refused. Group them into model classes, such as approved for passenger data and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Passenger and shipment data must never leave the building.	Argent runs entirely inside your walls, even on a fully air-gapped network. The install bundle is checked at every step as it crosses into your closed network.

WHAT REGULATORS ALREADY EXPECT

US DOT, 49 U.S.C. 46301. For airlines, up to **$75,000** per violation, each day counting again. DOT assessed one airline **$140** million after a holiday meltdown.[2]

EU GDPR, Articles 33 and 83. Tell the regulator within **72** hours of a breach, where feasible. The worst violations reach EUR **20** million or **4%** of turnover.[3]

HOW A CARRIER 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: customer 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 COMPANY'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026. 2 49 U.S.C. 46301 maximums, DOT notice, Federal Register, Jan 6, 2026; DOT Order 2023-12-11, Dec 2023. 3 Regulation (EU) 2016/679 (GDPR), Articles 33(1) and 83(5), EUR-Lex.