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

ARGENT FOR TELECOM CARRIERS

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 network. The FCC fined the nation's largest wireless carriers nearly $200 million over location data,[1] and one in four malicious breaches now uses AI.[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 CARRIERS ASK FOR FIRST

1	**Budget controls** A network agent runs up a large bill overnight.	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 care agent sends a caller's call history to an AI.	Argent reads each request first, tool results included, and blanks out phone, IP, Social Security and card numbers before anything leaves, plus your IMEI and SIM numbers once you add a pattern. The record notes the kind of data, never the data.
3	**Auditing for auditors** The regulator asks which agent saw call records.	Every AI decision goes into a signed, tamper-evident record that cannot be quietly changed. A regulator or internal audit can check a package of it on their own computer and see whether anything was altered.
4	**Model control** Staff 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 customer records and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Call records must never leave the building.	Argent runs entirely inside your own network, even a fully air-gapped one. The install bundle is checked at every step as it crosses into your closed environment.

WHAT REGULATORS ALREADY EXPECT

FCC CPNI rules, 47 CFR 64.2010. Carriers "must properly authenticate a customer prior to disclosing CPNI"; on a call the customer starts, call detail goes out only after a password.[3]

FCC fines, 47 CFR 1.80(b)(2). Up to $**251,322** for each violation or each day it continues, and up to $**2,513,215** for one continuing violation.[4]

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 CARRIER'S OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 FCC, News Release DOC-402213A1, location-data forfeitures, Apr 29, 2024. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, release Jul 29, 2026. 3 47 CFR 64.2010(a)-(b), eCFR, read 2026-11-19. 4 47 CFR 1.80(b)(2), eCFR, read 2026-11-19.