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

ARGENT FOR MANUFACTURERS

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. Manufacturing is the most attacked industry five years running,[1] and across industries, 43% of incidents now involve AI nobody approved.[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 MANUFACTURERS ASK FOR FIRST

1	**Budget controls** A plant's maintenance 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 program or product line spends on AI.
2	**Data protection** An engineer pastes design notes into an AI.	Argent reads each request and blanks out your own part and drawing number patterns, plus card, bank account and Social Security numbers, before anything leaves (registered specifications too, where you switch them on). The record notes what kind of data, never the data itself.
3	**Auditing for auditors** A defense customer asks where controlled data went.	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** Engineers 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 engineering data and general use. A model can be swapped for an approved one without staff changing anything.
5	**Air-gapped** Drawings and process 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

DFARS 252.204-7012. A defense supplier must report a cyber incident within **72** hours of discovering it.[3]

ITAR, 22 CFR 127.10. Sending controlled technical data abroad can be a violation: up to the greater of **$1,271,078** or twice the value of the deal, per violation.[4]

HOW A MANUFACTURER 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: design 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 X-Force Threat Intelligence Index 2026, industry trends. 2 IBM / Ponemon, Cost of a Data Breach Report 2026, all industries, July 2026. 3 DFARS 252.204-7012, acquisition.gov, read 2026-11-13. 4 22 CFR 127.10(a)(1)(i), eCFR, read 2026-11-13.