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

ARGENT SOVEREIGN AI

YOUR AI, YOUR NETWORK, YOUR EVIDENCE. YOU DECIDE WHAT LEAVES.

Argent Strategic Intelligence is the gateway between your AI agents and the models they use, and it runs inside your own environment. Gartner predicts that by 2029 more than **90%** of EU organizations will have a digital sovereignty strategy, reaching across data, technology, operations and AI.[1]

Built air-gap first. The gateway, console, sensitive-data detector and signed records run inside, and the AI model can too, on local engines such as Ollama and vLLM. Argent's own services open no outside connection by default.

SEE.
Every agent request, inside your own walls.

PROVE.
Signed records on storage you choose.

STOP.
Unapproved models and sensitive data, before they leave.

HOW ARGENT GETS YOU THERE

1	**Runs where you choose** The network has no internet connection.	One Helm chart covers Amazon EKS, Azure AKS, Google GKE and self-hosted k3s or RKE2, plus a single-server bundle. A sealed network gets one signed bundle, checked file by file.
2	**Routes you approve** An agent asks for a model nobody approved.	Requests go only where your routes point: a local model, or an approved provider such as AWS Bedrock or Azure AI Foundry. Once enforced, model access is deny by default, so any other model is refused.
3	**Data masked before it leaves** A prompt carries a customer's account number.	The sensitive-data detector ships in the signed release with its language model built in. Social Security, card and account numbers are masked or blocked before the request reaches the model, per your policy.
4	**Your keys, your storage** Security asks who holds the provider keys.	Provider keys stay in your vault, such as HashiCorp Vault or CyberArk Conjur; by default agents never hold one. The evidence archive sits inside the install or on your own object-locked cloud store.
5	**Proof without trusting us** An examiner wants to check the records.	Each signed record names the provider the request went to and the region label of its record chain. Examiners check the evidence on their own machine.

WHAT THE RULES ALREADY ASK FOR

GDPR Article 44 (organizations subject to the GDPR). A transfer of personal data outside the European Economic Area, or to an international organisation, "shall take place only if" its transfer chapter's conditions are met.[2]

NIST SP 800-53, SC-7(5) (US federal systems). Deny network traffic by default and allow it by exception. Argent's own services open no outside connection by default.[3]

HOW A SOVEREIGN ROLLOUT STARTS

1. Install inside. Pick on premises, private cloud or your VPC; carry in the signed bundle for a sealed network.

2. Route and mask. Point routes at local or approved models, and set what sensitive data must be masked.

3. Watch, then enforce. See what each control would have done on your own traffic, then switch them on one at a time.

BOOK A DEMO. SEE ARGENT RUN INSIDE YOUR OWN NETWORK, UNDER YOUR RULES.

NYEDIS.AI/DEMO

Sources. 1 Gartner press release, Gartner Predicts Digital Sovereignty Will Be a Core Component of National Security Strategies by 2030, November 11, 2026. 2 Regulation (EU) 2016/679 (GDPR), Article 44, eur-lex.europa.eu. 3 NIST SP 800-53 Rev. 5, control SC-7(5) Deny by Default - Allow by Exception, csrc.nist.gov.