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

ARGENT AIR-GAPPED INSTALL

YOUR NETWORK STAYS SEALED. ARGENT RUNS INSIDE IT.

Argent Strategic Intelligence sits between your AI agents and the models they use. It was built air-gap first: the gateway, the signed records, the sensitive-data detector and the console run inside your own network, and the AI model can too, on local engines such as Ollama, LM Studio and vLLM.[1]

Nothing is switched on that needs the internet. Argent's own services open no outside connection by default, and the console loads nothing from outside. Where the company allows it, the gateway also reaches outside AI providers.

SEE.
Every agent request, inside the sealed network.

PROVE.
A signed record of each one, stored inside.

STOP.
Sensitive data is stopped before the model.

FIVE THINGS THAT RUN INSIDE YOUR WALLS

1	**Gateway and records** An analyst's agent asks a local model about a loan file.	Every request from an agent that works through Argent passes the gateway, which checks it, passes it to the model and writes a signed, tamper-evident record. The evidence archive sits inside the install by default.
2	**Local AI models** The bank runs Ollama on its own servers.	Routes can point at self-hosted engines such as Ollama, LM Studio and vLLM, each turned on by an admin. Argent needs no AI model of its own to do its job.
3	**Data protection** A request carries a customer's Social Security number.	The sensitive-data detector ships inside the signed release with its language model built in. A request carrying sensitive data is masked or blocked before it reaches the model, per your policy, with no outside lookup.
4	**Signed bundle install** The release arrives on removable media.	One signed bundle carries every image, each pinned by digest, the Nyedis-built ones signed. The import checks the release signature, the checksum list, every file and each image's digest, stops on any mismatch, and loads your own registry.
5	**Outbound by choice** Security asks: does it phone home?	Argent's own services open no outside connection by default. The price feed is off until an operator turns it on, and connectors exist only when an admin adds them; an allowlist can make their traffic deny-by-default.

WHAT THE SECURITY STANDARDS SAY

NIST glossary (CNSSI 4009). An air gap is an interface where two systems are not connected physically and data moves "only manually, under human control."[1]

NIST SP 800-53, SC-7(5). For US federal moderate- and high-impact systems: deny network traffic by default and allow it by exception.[2]

HOW A TEAM STARTS

1. Carry in. Bring the signed bundle across on media. The import checks the signature and every file, then checks each image against its pinned digest as it loads it into your registry.

2. Install. One setting points the Helm chart or the single-server bundle at your registry.

3. Route. Point agents at the gateway, and routes at your local models or approved outside providers.

BOOK A DEMO. SEE ARGENT RUN INSIDE A NETWORK WITH NO INTERNET.

NYEDIS.AI/DEMO

Sources. 1 NIST CSRC Glossary, air gap (CNSSI 4009-2022, from IETF RFC 4949), csrc.nist.gov/glossary/term/air_gap. 2 NIST SP 800-53 Rev. 5, Security and Privacy Controls, control SC-7(5) Deny by Default - Allow by Exception, csrc.nist.gov.