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

ARGENT OFFBOARDS AGENTS

WHEN SOMEONE LEAVES, THEIR AGENTS STOP. THEN THEY GET A NEW OWNER.

Argent Strategic Intelligence puts a checkpoint between your AI agents and the AI services and tools they use. Every agent has a named human owner, checked on every request. With Identity Governance in enforce, when the owner leaves, the agent's very next request is refused and nothing reaches the AI model.

Agents outlive the people who built them. IBM found **92%** of organizations with an AI-related breach lacked proper AI access controls.[1] Argent's Org chart shows every agent that has lost its owner and why, and an admin hands each one to an active, accountable person.



SEE.
Every agent that has lost its owner, and why.



PROVE.
A signed record of every disable and reassign.



STOP.
A leaver's agents are refused on the next request.

FIVE THINGS TO KNOW ABOUT THE LEAVER FLOW

1	**Refused, not deleted** Rachel left; her loan agents still get work.	Once the owner is inactive, the agent's next request is refused and nothing reaches the model. Agents and keys are kept; the work waits for a new owner.
2	**Directory leavers** Rachel is removed in Microsoft Entra.	Connect Okta, Microsoft Entra, Auth0, Keycloak, LDAP directories or SQL databases (JDBC). Argent switches the person off at its next check and holds their agents' keys until a SuperAdmin releases them. Other identity tools can push over SCIM.
3	**The Org chart** The CISO asks which agents are orphaned.	Each agent whose owner left reads "Refused at every request since <name> left", with refusals in 24 hours. The person's status says why.
4	**Reassign** Her team still needs that work.	REASSIGN suggests a successor: the department's admin, then the organization's, then the team. Several agents move together in one signed change to an active owner.
5	**Signed and sticky** An admin disables a contractor by hand.	Disable, directory deactivation and reassign are each signed before they take effect. A console disable holds until an admin enables the person, whatever the directory says. A leaver's Argent console account, if any, stops too.

WHAT GOOD PRACTICE ASKS

NIST SP 800-53, control PS-4. On termination, "disable system access" and "retain access to organizational information and systems formerly controlled by terminated individual."[2]

NY-regulated financial firms. 23 NYCRR 500.7 requires covered entities to "promptly terminate access following departures."[3]

HOW A TEAM STARTS

1. Connect. Route agents through Argent and connect your directory under Identity sources.

2. Enforce. Watch the owner check first, then switch Identity Governance to enforce. A directory leaver's agents are held either way.

3. Reassign. Hand each orphaned agent to an active owner from the Org chart, with a signed record.

BOOK A DEMO. WE WILL SHOW YOU THE LEAVER FLOW WORKING ON YOUR OWN USE CASES.

NYEDIS.AI/DEMO

Sources. 1 IBM / Ponemon, Cost of a Data Breach Report 2026, July 2026 (602 organizations, March 2025 to February 2026). 2 NIST SP 800-53 Rev. 5 (Update 1), control PS-4 Personnel Termination, csrc.nist.gov. 3 NYDFS, 23 NYCRR Part 500 (Second Amendment, 2023), section 500.7(a)(6), dfs.ny.gov.