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

ARGENT KEYLESS AGENTS

AGENTS CARRY YOUR AI KEY TODAY. KEEP IT IN YOUR VAULT.

Argent Strategic Intelligence keeps your company's AI provider key in one place you control: the vault you already run, or Argent's own built-in vault. By default, the agents that work through Argent never hold that key. Each one holds its own Argent key instead, so a copied settings file no longer copies the key to your AI account.

The gateway attaches the key on the way out. Argent checks that the agent may use the key, fetches it from the vault, removes any provider key the agent sent and attaches the right one. If any step fails, the request is refused and nothing goes out. Every decision goes on a signed record that never contains the key.



SEE.
Which agent used which key, and when.



PROVE.
A signed record: agent, provider, vault path.



STOP.
Kill one agent; every other agent carries on.

FIVE CONTROLS IN ONE PLACE

1	**Your vault** The AI key sits in fifty settings files.	The provider key lives in your own vault (HashiCorp Vault or OpenBao, AWS Secrets Manager, CyberArk Conjur, Infisical) or in Argent's built-in vault. With your vault, Argent keeps a reference and resolves it on use; it never stores a copy of the value.
2	**One key per agent** A developer sets up a new coding agent.	Each agent gets its own Argent key, shown once, and points its AI client at the Argent gateway. The key tells Argent which agent is calling, and it stops at the gateway: the AI provider never receives it.
3	**Attached on the way out** An agent sends the company's key anyway.	Argent checks that this agent may use the credential, fetches the key from the vault, removes any provider key the agent sent and attaches the vault's key. Only agents allowed to use a credential get it.
4	**Refused, not sent** The vault cannot be reached one morning.	No credential on file, a vault that cannot be reached, an empty secret or an agent without permission: the request is refused with a named reason. A failed vault never falls back to the agent's own key.
5	**Stop one agent** One agent of fifty goes wrong.	An admin kills, quarantines or pauses that agent, or rotates its Argent key: the old key stops on the agent's next request. The company's provider key stays untouched in its vault, and every other agent carries on.

WHY IT MATTERS NOW

AI key leaks are surging. 1,275,105 AI-service secrets leaked on public GitHub in 2025, up **81%**, and more than **64%** of secrets found valid in 2022 still worked in January 2026.[1]

Leaked keys widen what agents can do. OWASP's Top 10 for Agentic Applications warns that leaked credentials let agents operate far beyond their intended scope.[2]

HOW A TEAM STARTS

1. Connect. Point Argent at the vault you already run, or use its built-in vault, and add the provider key once.

2. Register. Give each agent its own Argent key and point its AI client at the gateway, then retire the copies.

3. Prove. Every request leaves a signed record naming the agent, the provider and the vault path, never the key.

BOOK A DEMO. WE WILL SHOW YOU ARGENT ATTACHING YOUR AI KEY FROM YOUR OWN VAULT.

NYEDIS.AI/DEMO

Sources. 1 GitGuardian, The State of Secrets Sprawl 2026, March 2026, blog.gitguardian.com, read 2026-11-19. 2 OWASP GenAI Security Project, OWASP Top 10 for Agentic Applications (ASI03 Identity and Privilege Abuse), December 2025, genai.owasp.org.