WORKLOAD IDENTITY FEDERATION

aembit

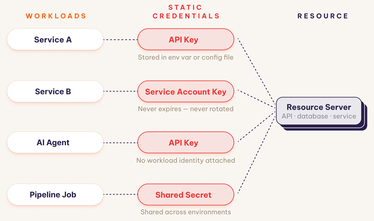
What is Workload *Identity Federation*?

How it enables secret-less identity & access for AI agents and machine workloads.

01 / 05 THE PROBLEM

Static Credentials Are the Risk

Most workloads authenticate using long-lived secrets — API keys, service-account keys, shared secrets — stored in config files, environment variables, or pulled from a vault. The secret still exists, and wherever it exists, it can be stolen.

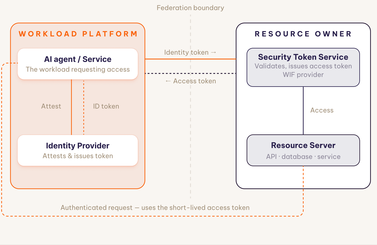


Even vault-retrieved secrets are static at the point of use — the workload still needs a secret to get the secret. Any exposed credential grants access with **no way to know which workload used it, or when**. Rotation is manual and risky, so it rarely happens. The blast radius of a breach is everything that credential could reach.

02 / 05 HOW WIF ELIMINATES THE SECRET

Two Trust Domains, One Boundary

With Workload Identity Federation, a workload proves who it is to its own platform's identity provider, then presents that proof across a federation boundary to a Security Token Service on the resource owner's side. The STS validates the identity token and issues a **short-lived access token** in return — no shared secrets, no pre-provisioned credentials. Every access request now carries a verified identity rather than a stolen or leaked key.

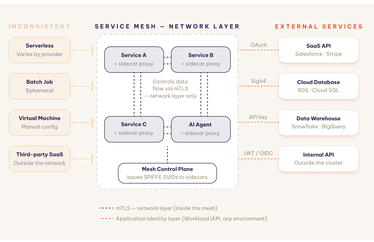


03 / 05 COMPLEMENTARY LAYER

What Service Meshes Do — And Don't Do

Service meshes are often seen as an alternative, but they solve the credential problem in one specific place. A mesh like Istio or Linkerd operates at the **network layer** — controlling traffic between workloads via mTLS inside a consistent environment such as a cluster. It does not authenticate workloads to external resources or broker access across different environments and credential types. Workload IAM operates at the **application identity layer** and is built to do exactly that.

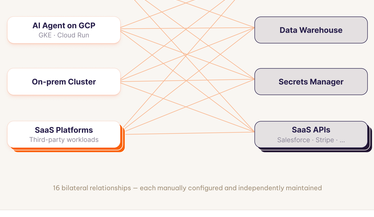
> Service mesh and Workload IAM are **complementary, not interchangeable**. The mesh handles network-layer traffic control inside the cluster; Workload IAM handles application-layer identity and access across any environment, for any credential type.



04 / 05 THE PROBLEM AT SCALE

Relationship Sprawl

WIF solves the credential problem — but not the configuration problem. Every workload platform must establish a **bilateral trust relationship** with every resource owner. At scale this becomes unmanageable: a burden for developers building software, and for security teams auditing access.



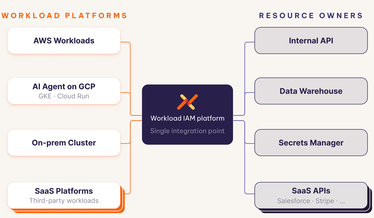
16 bilateral relationships — each manually configured and independently maintained

05 / 05 THE SOLUTION AT SCALE

A Workload IAM Platform as the Hub

A Workload IAM platform replaces the tangle with a **single integration point** on each side. Each workload platform integrates once. Each resource owner integrates once. Policy, audit, and access are managed centrally.

> ✓ Adding a new workload platform or resource owner takes **one new integration** — not new bilateral trust relationships, configurations, and policies.



Each side integrates once — policy, audit, and access managed centrally

aembit

Want to See Workload IAM *In Action*?

Aembit is the Workload IAM platform built for agentic AI and machine-to-machine access. No secrets. No sprawl. Just verified identity at every hop.

Request a demo at **aembit.io**