aembit

The Workload Identity & Access Management Platform

Aembit's Workload IAM platform secures access between workloads everywhere.

Secure Workload Access

Aembit Workload IAM provides policy based, contextual, and secretless access between workloads everywhere.

Simply & Centrally

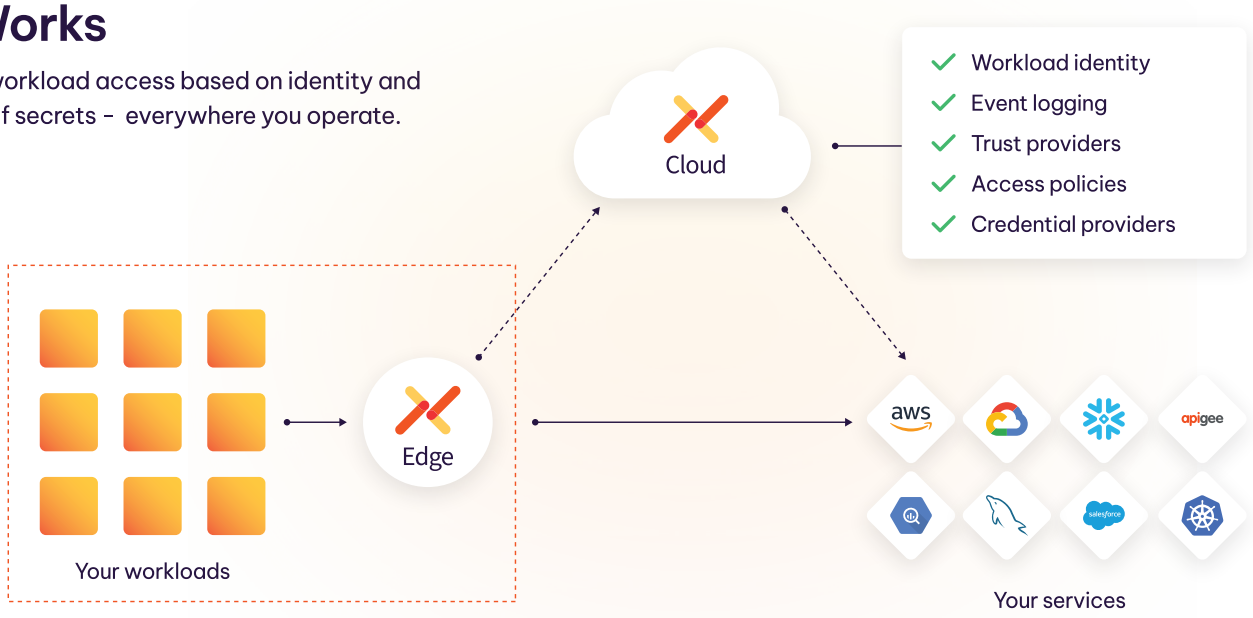
DevOps and Security have a single place to implement, manage, and log access, with no developer burden through no-code auth.

Across Environments

A single Workload IAM platform so your workloads can interact across clouds, SaaS services, and 3rd party APIs.

How it Works

Aembit secures workload access based on identity and policies instead of secrets - everywhere you operate.



Aembit Cloud

The Aembit Cloud is the policy system that brokers access rights between workloads across environments. Set, enforce, and log all access policies through Aembit. With every request, the Aembit Cloud verifies the client workload identity, and its access policy, and dynamically provides a credential trusted by the service. Aembit federates with the workload's environment to verify client identity, and with the service to issue credentials.

Aembit Edge

Aembit Edge is a transparent proxy, easily and scalably deployed through automation alongside each app. Aembit Edge makes implementation of workload identity simple, consistent, and robust with no coding required. It intercepts access attempts and then queries Aembit Cloud. Once authorized by Aembit Cloud, the Edge injects credentials into validated requests.

Capabilities

Centralized Access Policy

TODAY:
Teams leverage a spreadsheet of secrets, a secret manager, and a policy system for each cloud.

WITH AEMBIT:
You have a global policy system that allows you to define and enforce access policies between workloads in and across multiple environments.

Secretless Workload Authentication

TODAY:
To identify a workload today, the client workload stores an identity secret or a certificate. It's hard to bootstrap into this secret, and the secret must be protected against compromise, loss, or reuse.

WITH AEMBIT:
Aembit uses client environment attestation for Secretless Workload Authentication. The client no longer needs a long-lived identity secret, and access is enforced end-to-end.

Borderless Access

TODAY:
Security and DevOps teams must use multiple tools for different environments to achievetheir security goals. This is manual, slow, and frustrating, and leads to gaps which create security risks.

WITH AEMBIT:
Aembit gives you a single uniform way to work across clouds, SaaS services, and 3rd party APIs by creating credential providers for multiple services and environments.

No-code Auth

TODAY:
Implementing workload-to-workload access today requires a developer to code auth functionality within the app. It's time consuming, frustrating, inconsistent, and error prone.

WITH AEMBIT:
Aembit removes the burden of coding auth, while ensuring that Identity and Access Management is implemented effectively everywhere. It works for existing workloads with no code changes.

Logging

TODAY:
Logging for application access is distributed and inconsistently structured across workloads.

WITH AEMBIT:
Aembit logs access attempts in a single format, giving you pre-packaged queries to simplify audit, logging, and incident response. Easily view logs in Aembit or your SIEM.

Discovery

TODAY:
Determining communications among workloads is a manual process that requires developer involvement.

WITH AEMBIT:
Deploy Aembit in discovery mode to learn which applications your workload is connecting to, without modifying any access requests.

Use Cases

Secret Sprawl & Credential Rotation

With Aembit, applications no longer need to hard code sensitive credentials, or even request long-lived ones. Credential rotation is automated because client applications get a dynamic credential regularly.

Secrets Management

Instead of managing low level secrets, implement a Workload IAM platform that allows your team to focus on managing access. Aembit drastically simplifies access by eliminating the need for devs to code authn while improving overall workload security and visibility.

Secure Access to SaaS Services & 3rd Party APIs

Aembit provides a centralized and secretless method to authenticate to a broad array of services beyond your own workloads. Easily connect to services such as Snowflake, Stripe, BigQuery, Microsoft Graph, Apigee anddozens more.

Workload Zero Trust

Just like Zero Trust for users depends on a strong User IAM foundation, Zero Trust for workloads requires Workload IAM. With Aembit, you also can use posture signals from tools like Crowdstrike and Wiz to enforce conditional access policies.

"Secret Zero"

Aembit enables you to effectively bootstrap new, never-before-seen workloads into your environment without the need for an identity secret for the workload.

Auditing & Compliance

Aembit simplifies audit with a detailed, centralized log of access requests between client and target workloads. Aembit automates compliance with powerful built-in credential rotation.