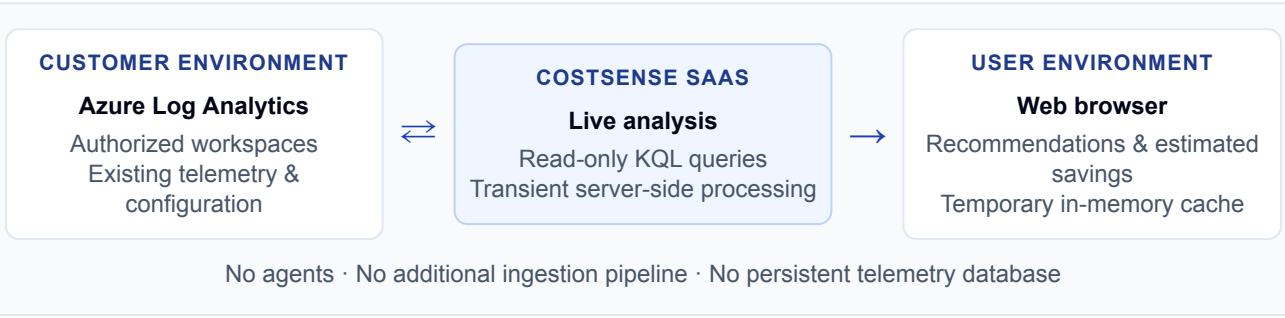
ARCHITECTURE & ACCESS

Secure cost optimization without moving your logs.

costSENSE analyzes Azure Log Analytics usage through live queries, delivering actionable optimization recommendations without using AI, agents, ingestion pipelines or persistent storage of queried telemetry.

Your logs remain in Azure Log Analytics.
costSENSE queries authorized workspaces on demand, processes results transiently and does not persist queried log data in its application database.

01 / How it works



No agents · No additional ingestion pipeline · No persistent telemetry database

02 / Authentication & Azure access

User sign-in

Users authenticate with their Microsoft identity via OAuth. costSENSE does not collect or store Microsoft account passwords.

Microsoft OAuth

Workspace connection

Customers configure a Microsoft Entra service principal to authorize access to selected Log Analytics workspaces. The associated secret is stored encrypted.

Customer-controlled access

Required permissions

Workspace access uses the **Log Analytics Reader** and **Privileged Log Analytics Reader** roles. These enable querying, including potentially sensitive log data; they do not grant permission to change workspace settings or delete logs. Access should be scoped to the workspaces being analyzed.

Read-only operations · Workspace-level scope · Revocable in Azure

Scope of access. costSENSE executes KQL queries and produces recommendations. It does not automatically apply configuration changes, modify retention policies, or delete customer telemetry.

DATA HANDLING & CONTROLS

Designed for minimal data retention.

Analysis happens on demand. costSENSE stores only the account, connection and subscription information needed to operate the service. It does not store a copy of your Log Analytics telemetry.

03 / What is processed and stored

DATA CATEGORY	HANDLING
Log Analytics query results	Processed transiently by the application backend and returned to the browser. Not persisted in the application database.
Analysis results in browser	Cached in browser memory for up to one hour.
Recommendation status	“Done” and “not relevant” selections are saved in the browser’s local storage.
Account information	Email address and account creation date are stored to operate the service.
Azure connection details	Tenant and service-principal identifiers, encrypted service-principal secret, and credential-validation metadata are stored.
Marketplace subscription	Subscription identifier and status are stored for subscription management.

04 / Disconnecting costSENSE

01 · DELETE ACCOUNT

Remove account

Deleting the costSENSE account removes its active account and configuration records.

02 · REVOKE AZURE ACCESS

Remove permissions

Revoke the service principal’s Azure role assignments and credentials in your tenant.

03 · NO LOG ARCHIVE

No telemetry export

There is no separate costSENSE log dataset to retrieve or purge from the application database.

Note: Account deletion describes active application records. Applicable infrastructure backup and operational log retention may follow separate retention schedules. Browser-local data is controlled by the browser and device.

Questions about architecture or security?
We’re happy to discuss your Azure setup and access requirements.

costsense.cloud ↗