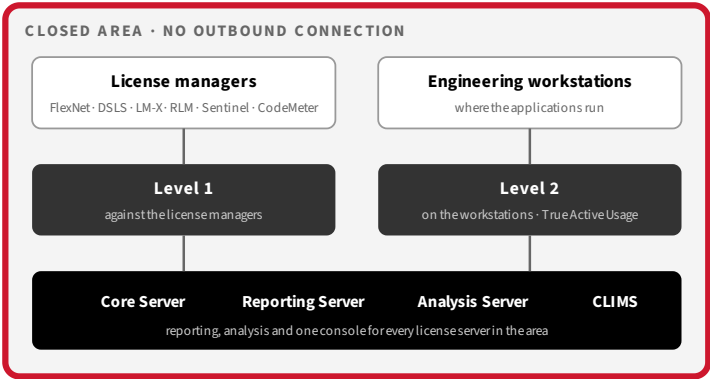


The Air-Gapped ESAM Architecture Guide

What runs inside the boundary, what can cross it, and who decides.

A tool that meters inside the enclave and analyzes in a cloud service isn't an air-gapped tool. Open iT installs as a self-contained deployment inside a closed area. Collection, reporting and analysis all run within the boundary, so nothing has to cross it for the system to work.

1 What runs inside the boundary



Four things install in the area and talk only to each other:

- **LicenseAnalyzer™ Level 1** (Runtime Usage) against the license managers.
- **Level 2** on the workstations, for True Active Usage.
- **CLIMS™** (Centralized License Integration and Management System) as the one console for every license server in the area.
- **The reporting and analysis servers** behind them.

Nothing calls out. A closed area gets metering, denial reporting and active-versus-inactive analysis on the same terms as your open network.

2 What can cross it: three data-handling patterns

Pattern	What leaves the area	When it applies	Who decides
Fully self-contained	Nothing. The area reports from inside itself.	Any closed area, including one with no path to the enterprise network.	Your security team
Periodic anonymized export	An anonymized data set, for consolidated reporting on the open side.	Only if your security governance allows an export.	Your security team specifies the export
Connected roll-up	Collected data, forwarded to a central server.	Only where a path already exists between an enterprise network and a program subnetwork.	Your security governance

Data Anonymization transforms user, host and application names while keeping the usage data reliable. Which pattern you get is a security-governance decision your team makes during implementation planning, not a product setting. Connected subnets roll up. Closed areas stay closed.

3 Who decides, and who touches the data

Activity	Your team	Open iT
Choose the data-handling pattern, specify any export	●	
Build and interpret reports, tune parameters	●	
Investigate denial patterns, produce renewal evidence	●	
Assign administrator and monitoring-only roles	●	
Set nationality or clearance rules for support staff	●	
Train your team to data analysis specialist level		●
Support and maintenance releases		●

In a classified environment we can't look at your data. That rules out the model where the vendor runs the analysis and hands over a report.

Instead, your team is trained on your system, with your data. They build and interpret the reports, tune parameters, investigate a denial pattern and produce the evidence a renewal needs, without anyone outside the organization seeing a record.

Where a program needs support staff of a particular nationality or holding a particular clearance, that gets agreed as part of the engagement rather than discovered afterwards.

Frozen baselines stay frozen

- Metering follows the license manager, not an application build, so it works whatever release sits behind it.
- Version data is captured in the record: three programs on three validated baselines read as three demand curves.
- Earlier releases keep receiving maintenance. Hotfix streams are maintained for 9.17, 9.19 and 10.1 across Core Server, client and CLIMS.

Assurance for the architecture review

- ISO/IEC 27001:2022 certified by BARR, across all Open iT products. Certificate: openit.com/iso-27001.
- Single sign-on through Microsoft Entra ID (SAML 2.0, multi-AD-group support) or Okta.
- Role-based access separates administrators holding full management rights from users with monitoring-only access.
- CLIMS records every license-management event, an audit trail the product documentation lists as relevant to regulated industries including aerospace and defense.

Start here: bring us the constraint, not the requirement. Which areas are closed, which baselines are frozen, what your personnel rules are, and which applications matter. Then run a Level 1 usage assessment across one renewal cycle. In a closed area it runs entirely inside the boundary.