

Security architecture, at a glance

Explicit permissions, outbound-only connectivity and tenant-scoped access.



1 What is installed

One lightweight Deployment, a dedicated ServiceAccount, read-only ClusterRole/Binding, connection Secret and optional egress NetworkPolicy. The SaaS platform does not require customer kubeconfig access.

2 Access and modification boundary

The published collector role uses explicit get/list verbs; optional pod logs use get. It has no create, update, patch or delete verbs. Generated commands and YAML remain review-first.

3 What leaves the cluster

Bounded health/state, CPU and memory observations, selected Kubernetes events, configured manifest summaries and—when enabled—limited current/previous container log evidence. Collection and payload limits are configurable.

4 Sensitive data handling

Secret values and Secret key names are never transmitted. With manifest collection enabled, only Secret existence, type and value counts may be summarized. ConfigMap values are excluded by default.

5 Authentication, authorization and audit

Password authentication and workspace OIDC/SSO are supported. Tenant scope comes from the authenticated identity. Roles, teams and cluster assignments control visibility; sensitive actions retain actor attribution.

6 Retention, deletion and evidence

Documented periods: snapshots 7d, raw metrics 14d, hourly rollups 90d, operational state/events 180d and sanitized incident evidence 30d. The dated benchmark records 14/14 controlled diagnoses.

IMPORTANT REVIEW BOUNDARY

Secret read permission and transmitted Secret data are different controls: the agent can verify that a Secret exists while excluding values and key names from its payload. This summary is not a certification, DPA or universal accuracy guarantee.