ONAM SECURITY

TECHNICAL WHITEPAPER · 04

Security & trust

How Onam connects, what it stores, what it never stores, and how tenants stay isolated — the trust case for a read-only platform.

Least privilege

No stored secrets

Metadata not data

Per-tenant isolation

SOC 2 · ISO · PCI

THE ARGUMENT, IN ORDER

00 Executive summary

A security tool has to earn more trust than it asks for.

Onam reads your entire cloud. That access is exactly why our own security posture has to be exemplary and legible. This paper documents how Onam connects, what it stores, what it deliberately never stores, and how tenants are isolated — so a security team can grant access with confidence rather than hope.

The design principle is minimality: take the least privilege that permits a security read, hold no long-lived secrets, and retain only the metadata needed to describe a risk — never the data itself. Where a control is a stated certification, it is named; where something is planned rather than achieved, this paper does not claim it.

> **The short version.** Read-only, agentless, short-lived tokens, per-tenant isolation with per-tenant keys, and a retention policy that keeps labels and locations but not contents. The rest of this paper is the detail behind each of those words.

01 Least-privilege connection

No long-lived cloud credential is ever stored — only a reference, exchanged for a token that expires within the hour.

Every cloud is connected with the lowest standing privilege that still allows a security read, and no long-lived cloud credential is ever stored — only a reference (a role ARN or principal ID) held in a secrets manager and encrypted with a managed key. At scan time that reference is exchanged for a short-lived token.

Cloud	Mechanism	Privilege
AWS	Cross-account role, unique External ID per tenant	SecurityAudit + ReadOnlyAccess; STS ≤ 60 min
Azure	Entra service principal	Reader + read-only Graph
GCP	Service account or keyless WIF	6 read-only roles
OCI	IAM user + signing key	inspect + read only
Alibaba / IBM	RAM read-only · Service ID	Read-only; key exchanged for short-lived Bearer
Kubernetes	Read-only ServiceAccount	get / list / watch

> **Confused-deputy defence.** The AWS connection requires a unique External ID per tenant, so one tenant's role can never be assumed on behalf of another. Tokens expire in an hour or less, and secret material is never written to logs.

02 What Onam never stores

The most important trust control is what does not enter the system.

Onam keeps the metadata required to describe and price a risk, and deliberately discards everything else.

This is what makes "we read your entire cloud" a bounded statement. Onam knows that a bucket holds restricted data and where it sits on a path; it does not hold the objects in it.

03 Tenant isolation

Isolation here is separate keys and separate execution, not a tenant column in a shared table.

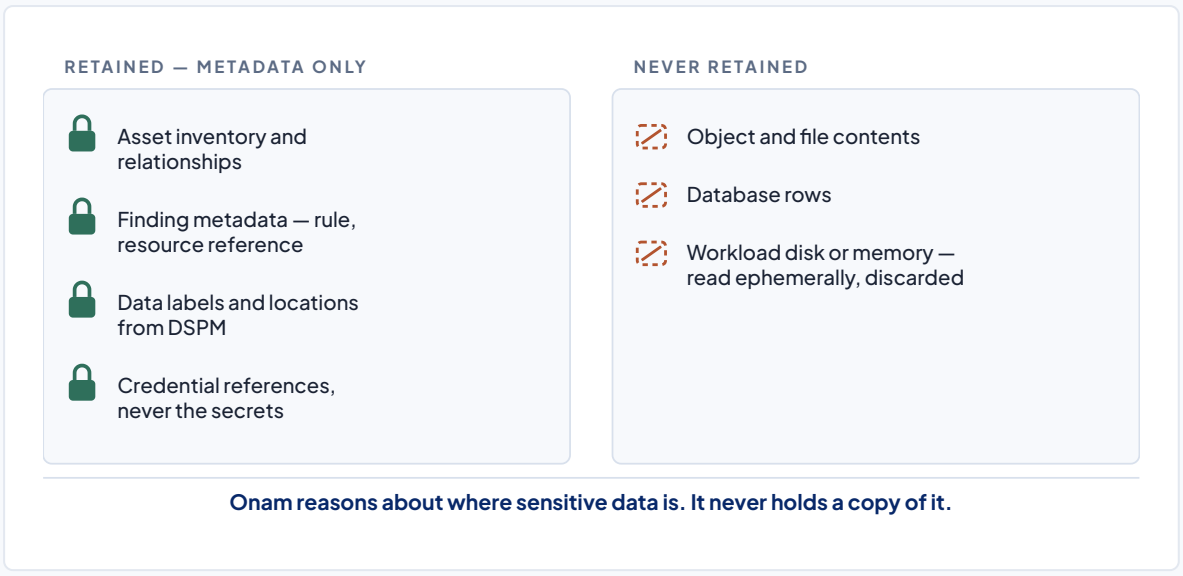

FIGURE 1 — RETAINED VS NEVER RETAINED

The right column is the commitment. Everything in it is read, used, and discarded in the same pass.

Each tenant's data is isolated with per-tenant keys, so a defect in one tenancy cannot expose another. Scan execution, storage and key material are separated per tenant rather than partitioned by a shared identifier in a shared store.

04 Agentless by design — and what that costs

Nothing is deployed on your workloads. There is no kernel module, no sidecar, no daemon to patch, and no agent fleet to roll out or roll back. Onboarding is a role grant, and removing Onam is revoking it.

> **The honest limit.** Agentless is a trade, not a free win. Onam has no live inline runtime enforcement: it evaluates posture continuously and detects from audit logs, but it cannot block a process on a host the way an agented product can. If inline blocking is a requirement, that requirement is not met by this architecture.

05 Certifications and claims discipline

Nothing on a roadmap is written in the present tense in this paper.

Where Onam holds a certification, this paper names it. Where a control is implemented but not certified, it is described as implemented. Where something is on a roadmap, it is labelled planned and never stated in the present tense.

That discipline is itself a security control: a trust document that overstates is a trust document that will be checked, disbelieved, and then discounted entirely.

06 Summary

Every claim in this paper is either a control you can inspect or a limit we state.

- Least privilege per cloud, with no long-lived credential stored — only a reference, exchanged for a token of an hour or less.
- Metadata is retained; contents are not. Labels and locations, never rows and objects.
- Per-tenant isolation with per-tenant keys.
- Agentless by design, and honest that this means no inline runtime enforcement.
- Present tense means shipped. Planned means planned.