Secure Isn't Sovereign: Why European Teams Are Rethinking Elasticsearch Encryption

Anja Glauch · 2026-05-21

Secure Isn't Sovereign: Why European Teams Are Rethinking Elasticsearch Encryption

Picture the scene. A regulated EU team has just walked an auditor through their Elasticsearch deployment. Authentication is hardened. RBAC is granular. The audit log survived a spot check. Everyone is relaxing into their second coffee when the auditor asks a quiet question.

Where do the encryption keys for your Elasticsearch translogs live?

The room goes quiet.

That pause is the gap between *secure* and *sovereign*, and in 2026 it is where most of the real compliance exposure now sits.

Secure and sovereign are not the same thing

"Secure" is about keeping the wrong people out. Authentication, TLS, role-based access control, perimeter hardening. These are table stakes in any serious production cluster. If you haven't done them, you don't have a cluster, you have an incident waiting to be written up.

"Sovereign" is a different question. It asks who *controls* the data, where it lives, and who holds the keys. It is the difference between being a good tenant and being the landlord of your own data.

You can be fully secure and only partially sovereign. Most EU teams running Elasticsearch today sit exactly there.

What EU regulation is actually asking for in 2026

The direction of travel across European regulation is unmistakable. NIS2 is in force and has meaningfully raised the bar for critical and important entities, with closer attention to supply-chain risk and cryptographic controls. The EU Cyber Resilience Act is phasing in, pushing obligations further upstream into the products and components organisations deploy. GDPR enforcement has continued to mature, with regulators paying more attention to processor arrangements and cross-border data flows than they did even two years ago.

These frameworks differ in scope and mechanism, but they converge on a single point. Data protection, on its own, is no longer enough. Regulators increasingly want evidence of data *control* — provable, auditable, and not contingent on a third party's goodwill.

That is a meaningful shift. Encrypting data "at some point, somewhere in the vendor's stack" used to be a defensible answer. It is becoming a much harder one to defend. Elasticsearch data sovereignty is moving from a nice-to-have architectural choice to a procurement-level requirement.

Where most Elasticsearch deployments quietly fall short

Three gaps tend to surface the moment a serious audit begins.

Keys held by the vendor. A vendor-managed KMS is operationally convenient, but it creates a dependency the data controller cannot unwind. If you don't hold the keys, you don't, in the strict regulatory sense, control the data. That is increasingly a problem in procurement reviews, and customer-managed encryption keys for Elasticsearch are becoming the expected baseline rather than an advanced option.

Unencrypted translogs. This is the one that catches even mature teams. Translogs are ephemeral by design, which is precisely why they get overlooked. They contain the full payload of recent writes, and anyone with disk access can reconstruct a surprising amount of recent history from translog files alone. Encrypting indices and snapshots while leaving translogs in the clear is a common and quietly serious compliance gap.

Audit trails that don't survive forensic review. Audit logging that records access events without the context around them — principal, tenant, document-level action, field-level visibility — will not hold up when a regulator asks *who saw what, when, and under what role.* You either have that picture or you don't.

None of these are theoretical. They are the questions that come up in the room.

What a sovereign-grade stack actually looks like

A sovereign-grade Elasticsearch stack has a recognisable shape. If you are putting together a checklist for your next architecture review, it looks roughly like this.

- **Encryption at rest across indices, snapshots, *and* translogs.** All three, not two out of three.
- **Customer-held encryption keys.** No hard dependency on an external KMS the vendor controls.
- **Fine-grained RBAC with document-level and field-level permissions.** Role boundaries that follow the data, not just the index.

- **Multi-tenancy for isolated workloads on shared clusters.** So separation of concerns doesn't cost you a second cluster.
- **Detailed audit logging.** Rich enough to reconstruct access patterns under scrutiny, not just show that logging exists.
- **Clearly documented data residency.** Where the data sits, where it moves, and what jurisdiction governs each hop.
- **Authentication that fits your existing identity estate** — LDAP, Kerberos, OpenID Connect, SAML — rather than forcing a parallel one alongside it.

If your current stack ticks five of those seven, you are in decent shape. If it ticks fewer, the conversation with your compliance lead is probably overdue.

A practical note on cost, because it always comes up. Predictable licensing matters here. Paying only for production clusters, leaving staging and test free, not being charged per additional node — that is what makes it realistic to run a properly sovereign architecture without the budget conversation becoming the blocker. Many European teams find the total cost of ownership lands 50 to 70 percent below what they were previously quoted for comparable enterprise tiers.

Why this matters now

The May content on this blog focused on implementation — authentication, RBAC, audit logging. That work is foundational. But it answers the "secure" question, not the "sovereign" one. The next layer is where 2026's compliance pressure is actually landing: key custody, and encryption at rest including translogs.

We'll be in Berlin in early June, on home ground. Search Guard has been built here since 2013 as a product of floragunn GmbH, and we will be hosting the Search Guard × OpenSearch Berlin Meetup on 5 June and demonstrating at Berlin Buzzwords from 7 to 9 June. If you would rather have this conversation in person, come and find us.

This article was published on the Search Guard blog: https://search-guard.com/blog/secure-isnt-sovereign-why-european-teams-are-rethinking-elasticsearch-encryption/