Application-Level Encryption at Rest Gains Attention in Elasticsearch Security Reviews

Search Guard discusses application-level Encryption at Rest for Elasticsearch, including Lucene files, snapshots, and translogs.

Search Guard

BERLIN, GERMANY, March 4, 2026 /EINPresswire.com/ -- As organizations expand their use of Elasticsearch for analytics, observability, and operational data workloads, security assessments are increasingly examining how stored data is protected beyond network-level encryption and infrastructure disk controls.

> Encryption at the storage layer is often assumed to be sufficient. However, search platforms introduce additional data handling layers that require independent review."
>
> *Jochen Kressin*

While many deployments rely on operating system or cloud-provider disk encryption, application-level encryption at the search engine layer is becoming part of compliance and internal security reviews — particularly in regulated industries.

Search Guard, a Berlin-based software company founded in 2013, has published details of its Encryption at Rest implementation for Elasticsearch. According to the company, the plugin-based approach encrypts three core storage components within Elasticsearch:

- Lucene data files, which contain indexed search data
- Snapshots, used for backup and archival processes
- Transaction logs (translogs), which record recent indexing operations

Translogs are of particular interest during security audits because they may temporarily store recently indexed sensitive data before it is fully committed to segment files. Security reviews increasingly evaluate whether this layer is explicitly protected.

Search Guard states that its implementation provides application-level encryption for Elasticsearch environments and is currently the only commercially available plugin designed to

encrypt Lucene files, snapshots, and translogs directly within the Elasticsearch process layer.

Encryption keys are managed externally and remain under customer control. Keys are not stored alongside encrypted data.

“Encryption at the storage layer is often assumed to be sufficient,” said Jochen Kressin, CEO of floragunn GmbH. “However, search platforms introduce additional data handling layers that require independent review. We are seeing more organizations examine how translogs and snapshot data are protected.”

The capability can be deployed in on-premises, private cloud, or public cloud environments and is compatible with containerized infrastructures including Kubernetes and Docker.

Search Guard develops security and compliance extensions for Elasticsearch deployments across sectors including financial services, healthcare, public administration, and SaaS platforms.

Further technical documentation is available at https://docs.search-guard.com/latest/encryption-at-rest-introduction.

Anja Glauch
Search Guard - floragunn GmbH
email us here
Visit us on social media:
LinkedIn
YouTube
