GDPR compliance for Elasticsearch

Jochen Kressin · 2020-09-14

The Search Guard Compliance Edition for Elasticsearch offers many specialized features that help you to make your Elastic Stack compliant with regulations like GDPR, HIPAA, PCI, ISO or SOX. In this article, we take a quick look at how you can use these features for GDPR compliance.

Least-privileges access principle

GDPR mandates that access to Personally Identifiable Information (PII) data like email, address, first name, and last name must be governed by strict access controls. You should always apply a least-privileges access principle. Access controls should enable authorized users to access only the minimum necessary information needed to perform job functions.

> GDPR mandates that access to Personally Identifiable Information (PII) data must be governed by strict access controls.

Search Guard provides role-based access controls to clearly define what Elasticsearch indices a user can access and what the user can do with the data.

Control access to PII documents and fields in Elasticsearch

If your index contains documents with PII data, then just governing access to that data is not enough. You also want to control what documents and what fields a user is allowed to see. For example, you may want to exclude any PII fields from an Elasticsearch query's documents.

If your index contains PII and non-PII documents, you may wish to exclude PII documents altogether. This is exactly what the Document-Level and Field-Level security controls provides: Filter out certain documents Elasticsearch that contain PII data, or blacklist or whitelist PII fields from existing documents

Elasticsearch field anonymization

Sometimes filtering documents and fields is not enough. You may still need to run analytics and statistics on PII data without seeing the data in cleartext. Search Guard can anonymize any data stored in Elasticsearch on-the-fly at runtime.

> Search Guard can anonymize any data stored in Elasticsearch on-the-fly at runtime

This means you can just index and store PII data as usual, and then decide afterward which users can see the data in cleartext and which other users can see the data anonymized. You do not need to decide at ingest time. And you can still use any feature that Elasticsearch provides, like aggregations.

Tracking access to PII data

Under GDPR, a user has the right to know who has accessed their PII data, when that was and for what purpose. Search Guard can monitor Elasticsearch queries that contain PII data and produce an audit trail whenever this PII data has been accessed.

A user can also demand information about what PII data has or had been stored. The Search Guard Write-History feature can monitor the complete lifecycle of an Elasticsearch document. This also includes how the document has changed over time. If for example, someone changes the email address of a customer, you can exactly tell when the change was made, by whom, and what the change looks like.

Right to be forgotten

Under the *right to be forgotten*

"[...] the GDPR gives individuals the right to ask organizations to delete their personal data. [...] The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay"

(https://gdpr.eu/right-to-be-forgotten/)

Search Guard can track all data deletions in Elasticsearch and store those events as an audit trail. You can always prove that PII data has actually been deleted, by whom, and when.

Data Integrity: Immutable Indices

Search Guard produces audit trails to conform to security regulations like GDPR. However, to ensure those critical audit events cannot be changed or tampered with after being created, you need to store them securely. For that, Search Guard offers the immutable indices feature. Documents, once written to an immutable index, cannot be changed anymore.

Summary

The Search Guard Compliance Edition offers a wide range of features that help you keep your Elasticsearch cluster and the entire Elastic Stack compliant with GDPR, PCI, HIPAA or SOX:

- Encryption for data in transit
- Support for encryption at REST
- Role-Based Access Control (RBAC) for any index
- Access control to PII documents and PII fields
- Data anonymization
- Data access tracking
- Data change tracking
- Immutable indices for data integrity

Where to go next?

Give the Search Guard Compliance Edition a spin. All downloads come with a free 60-day trial license.

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-gdpr/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial