Search Guard Compliance Features – Technical Preview

Jochen Kressin · 2018-01-24

Existing and upcoming security compliance regulations like GDPR, HIPAA, PCI DSS or SOX require a business to protect, track and control access to sensitive data. While Search Guard always had very strong compliance features like mandatory TLS encryption and audit logging, we will take that one step further with the upcoming Search Guard Compliance Edition. Download and try the first technical preview of our new compliance features today!

Security and Compliance first

Search Guard was always about putting security first. Search Guard the first Elasticsearch security plugin that made TLS on transport layer mandatory and was also the first plugin without any default users and passwords upon installation. We believe that networks, including internal networks, are inherently insecure. We believe that implementing security for REST only is not real security. And we also take care of not-so-obvious attack vectors like LDAP timing attacks or client-side TLS renegotiation. With the Audit Logging feature, you are able to monitor any access to data stored in Elasticsearch and track and store malicious events.

These are all great tools to help you stay compliant with regulations like GDPR, HIPAA, PCI DSS or SOX. However, we want to make it even easier for you to meet these regulations and thus will make compliance a first-class citizen in Search Guard as well.

Today we are releasing the first technology preview of the upcoming Search Guard Compliance Edition, geared specifically towards meeting compliance regulations. Take part in the Search Guard Vanguard programme and be the first to download and try our new compliance features!

Taking audit logging to the next level: Read and write history

The first technology preview contains two features that allow you to track both read and write access to sensitive data in your cluster, all the way down to the field level.

Read history audit logging

Compliance regulations are all about securing access to sensitive data. That could be patient data under HIPAA, personally identifiable information (PII) under GDPR, or financial data or credit card information under PCI DSS. Access to this data has to be secured and made available only for certain users for an intended purpose. But how do you know which user has actually accessed what data, and when?

With the new read history audit logging, you can exactly do that. Mark an index and fields in documents as *watched*, and Search Guard will produce an exact audit trail about who has accessed those *watched* fields. We do that not just on a document level but evaluate which fields were actually returned to the user. In other words, if those fields are filtered, for example by source filtering or field-level security, no events are emitted. So if Search Guard records a *READ* event, you can be sure that it was actually returned to the user in the search result.

For example, under GDPR, you can generate an audit trail and log which employee has accessed what PII information of your customers or users. Simply enable read history, mark all PII fields as *watched*, and ship the generated *READ* events to a storage of your choice. Or, if you face a data breach, you can exactly see when the data was accessed, and by whom.

Read more about the setup and configuration of the read history on our official docs.

Write history audit logging

Similar to the read history Search Guard can also keep an audit trail about write history. This, of course, includes the obvious cases of *CREATE* and *DELETE* operations. You can exactly monitor when for example PII data for a particular customer or user was created. More importantly, you can also monitor and store when this data was deleted. This is required under GDPR where a customer can demand deletion of his personal data and get confirmation that the data has actually been deleted. With the Search Guard write history feature you can now monitor and store exactly this information. But it does not stop there!

Recording changes to documents

Data changes over time. In Elasticsearch, technically speaking, this means that if you update a document the existing data is deleted and the new data is indexed. In other words, you do not know what a particular document looked like before the update. Search Guard can track and store any changes to your documents, including changing, adding or deleting fields. Need to prove that a customer's email address has actually been deleted? Need to verify when a PII field has been changed, and what the new value is? Search Guard gives you just that.

Any change to a document is stored in JSON patch format, so you can see which fields have been changed, added or deleted:

```
[
 {
   "op": "remove",
   "path": "/date"
 },
 {
   "op": "replace",
   "path": "/revenue",
   "value": 67000
 },
 {
   "op": "remove",
   "path": "/customers"
 },
 {
   "op": "add",
   "path": "/remarks",
   "value": "none"
 }
]
```

Read more about the setup and configuration of the write history on our official docs.

Roadmap

These are only two new features of the Search Guard Compliance Edition. There is much more to come, so stay tuned! We will release technology previews of our other features as well and release the GA version in Q1 2018. The immediate next features will be geared towards monitoring the integrity of your Elasticsearch installation.

If you have any questions, drop us a note and we're happy to help.

Search Guard Vanguard

We need your input and feedback! If you have 5 minutes time, please take part in our Search Guard Vanguard survey and let us know what your specific requirements regarding compliance are. Not only can you help us shape the new compliance features to your needs, we are also giving away a Search Guard license for free in our sweepstake. And if you like we will also keep you up-to-date about the compliance roadmap.

Become a Search Guard Vanguard by answering the compliance survey

Where to go next

- Download and install the Search Guard compliance technical preview
- Learn more about the read history audit trail by studying the official docs
- Learn more about the write history audit trail by studying the official docs
- Become a Search Guard Vanguard by answering the compliance survey

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