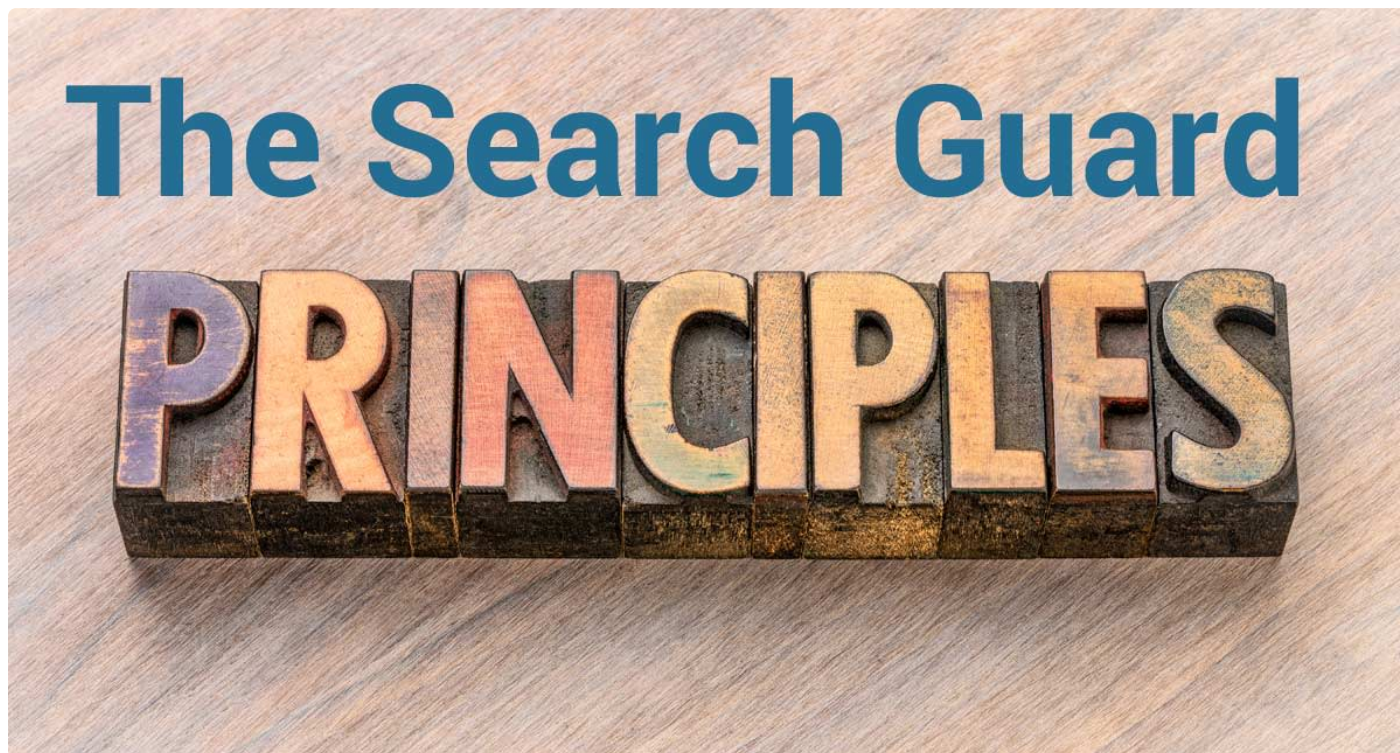


The Principles Behind Search Guard

Claudia Kressin · 2022-11-11



Search Guard has always been a pioneer in providing enterprise security for Elasticsearch. At the same time, we also strive to provide the best licensing model and give back to the community.

When shaping the business model behind Search Guard in 2015 and evaluating the market, we quickly came to the conclusion that there were practically no good offerings. So we thought about what we as users would like to see in such a security product for Elasticsearch.

Open Source and Open Code

Security is a vital part of any IT infrastructure. Data breaches happen all the time and cost you money, customers, and reputation.

Our standpoint was, and still is, that [Security has to be Open Source by definition](#). As a user, you need to have the ability to inspect and audit the security code you are running. Closed-source solutions, such as competitor products at the time, are a no-go.

Consequently, the [complete code of Search Guard](#), including the [commercial modules](#), was always publicly available for you to download, inspect, and audit. You can also compile Search Guard on your own infrastructure if you don't want to install binaries provided by a third party.

Fundamental Security Features Need to be Free

A software solution without any built-in security layer cannot be used safely in production. That's a given. In case users are charged for even the most basic security features the result will be [data breaches](#), [lost](#)

data and exposed systems.

Search Guard's Security for Elasticsearch was always free

Search Guard always offered the [Community Edition at absolutely no charge](#). The Community Edition already comes with a wide range of features like encryption, authentication, authorization, and role-based access control for Elasticsearch and Kibana. [Search Guard's Security for Elasticsearch was always free](#).

A Sane Licensing Model

While a licensing model that works for end users must be simple, affordable, and straightforward a company can only survive if it is able to pay its staff. However, nothing is worse than having to revisit your licensing plan often and pay more and more once your data size grows.

Scale your cluster, not your cost

We decided not to provide a volume-based licensing model with our Enterprise features. Instead, we license Search Guard per production cluster. The amount of nodes is irrelevant. You can scale your cluster to infinity without any additional cost. Non-productive systems like staging, development, or QA are included in the license, free of charge.

Security First

When designing the architecture of Search Guard a main goal was to make sure we put security first. We did not want to take any shortcuts: While the user experience is definitely significant, a reliable security layer is paramount. We do not believe in "one-click" security solutions that can be installed and configured without a fair amount of technical security knowledge. Do not trust anyone telling you otherwise.

Unlike other security products for Elasticsearch, we never had any default users and passwords baked into Search Guard, like the dreaded `admin/admin` account. We all know those default accounts never get changed and pose a significant risk on production systems.

So we made TLS encryption on transport layer mandatory, always. You have to get familiar with TLS, at least on a conceptual level, to install and use Search Guard. Why? Because without transport encryption, all other security features are pretty useless: All your traffic can be sniffed. [Remember, more than 60% of all attacks originate from the inside of your network, not the outside.](#)

Quality Control: Verified by Veracode

But we also do not want you to simply trust our words when it comes to security. We decided early on that we also want to have our code checked by a renowned and independent third party: Search Guard is [verified by Veracode](#). We use the Veracode platform to analyze and [scan every Search Guard version](#) and all used third-party libraries for security issues before release.

Giving back to Science and Education

Another thing that is very important to us is giving back to science and education. We believe that science and education are of utmost importance for the solution of current and future problems.

We always offer free licenses for non-profit educational and scientific companies and projects.

We always offered [free Search Guard Enterprise and Compliance licenses](#) for non-profit educational and scientific projects. And we will continue to do so. To apply for an Academic license, just [head over to our contact page](#) and drop us a note!

A big Thanks to all our Users and Customers

Our learning from the past years is: Building a business model that serves our users and customers best, and at the same time allows us to constantly work on and improve Search Guard is not an easy task. But if you put a lot of hard work, dedication and effort into it, it can be done. And once you have your core principles and values set up, stick to it. We hope the result of our efforts are of value to you, our users and customers. Thank you very much for supporting us in the last years! If you have any feedback about Search Guard or our business model, positive and negative, just [let us know](#)!

This article was published on the Search Guard blog: <https://search-guard.com/blog/search-guard-principles/>
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · [Start a free trial](#)