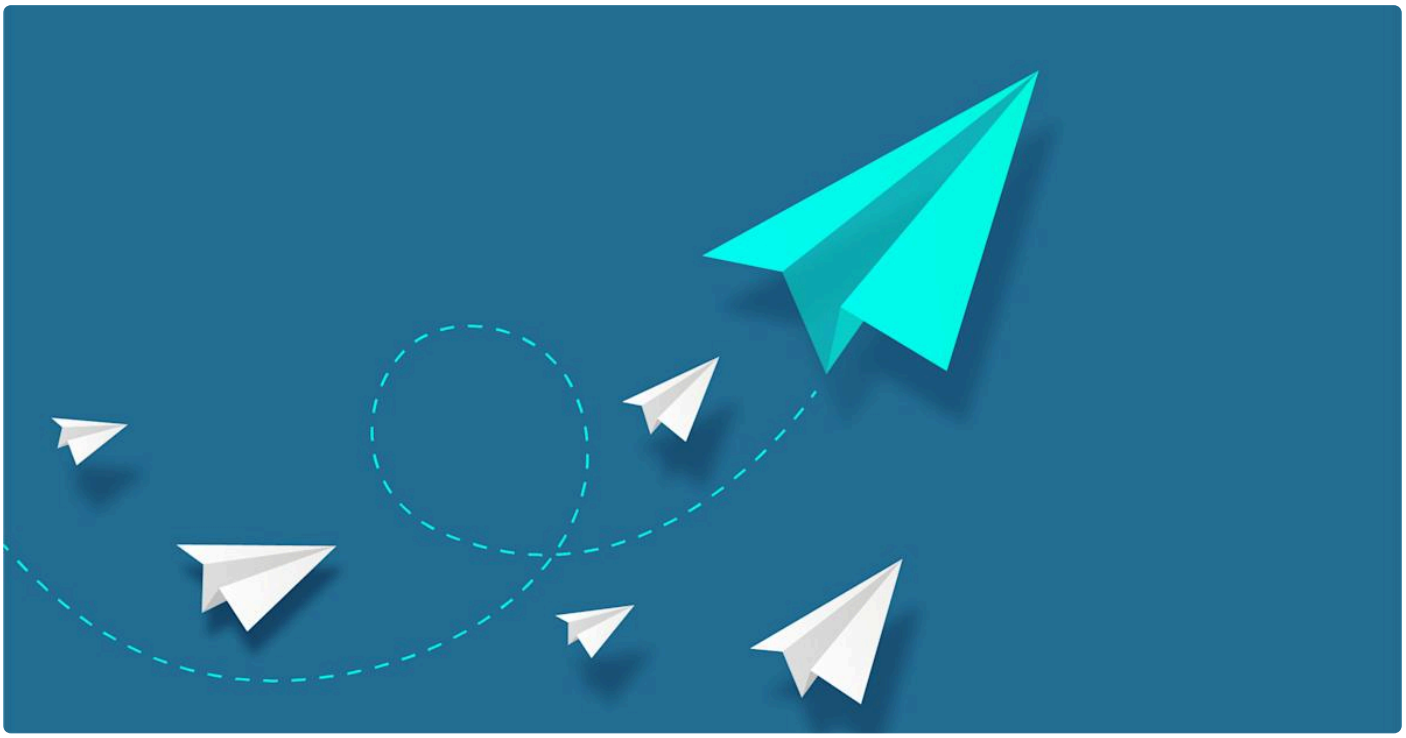
Security for Elasticsearch was always free with Search Guard

Jochen Kressin · 2019-05-28



We all love Elasticsearch as software. Despite one very fundamental drawback it had in the beginning: No free security-related features whatsoever. Many vanilla Elasticsearch installations were wide open for attacks. Some still are today, leading to massive data breaches over time.

Security first and done right

Any software without a security layer is not production ready. Sadly, we all know that security comes last in most software and infrastructure projects. Not providing any built-in security controls inevitably leads to data breaches and exposed data.

Following the zero-trusted-networks approach, we believe that

- security has to be implemented where the data lives
- any data that moves across the wire has to be encrypted

> Software without a security layer is not production ready

You, as a user, should not be responsible for implementing access control and data encryption yourself. Our mission is always to put security first and provide you with the best security features for Elasticsearch available.

Pioneers in Elasticsearch security

While there had been a couple of GitHub pull requests around security and TLS, Elastic used to have the opinion that security does not belong into Elasticsearch core and that ''the value [of TLS], security wise is close to 0''.

Our view on security for Elasticsearch has always been fundamentally different: Any software that stores potentially sensitive information has to have a security and access layer built-in.

We started to work on Search Guard early in 2013, un-creatively called “Elasticsearch Security Plugin” back then. The release of Shield 1.0 did not happen before February 2015.

Elasticsearch security, for free, and Open Source

Since the initial release of Search Guard, we always provided a free Community Edition at no cost, licensed under Apache2, which covers all major security features required to run Elasticsearch in production safely:

- Role-based access control on index- and document type level
- Internal database of users, roles and permissions
- Mandatory TLS inter-node encryption
- REST layer TLS encryption
- HTTP Basic authentication
- Kibana access controls

The Community Edition offers a full feature set to mitigate almost all attack vectors, including ransomware attacks and data leakages. So there was no reason anymore to run an unsecured Elasticsearch cluster in production.

For users who need more, we offer the commercial Enterprise Edition, with advanced features like LDAP, Kerberos, SAML, Document- and Field-level security and a lot of features around compliance, for a fair price.

> As the pioneers in securing Elasticsearch clusters, all decisions about our technology have the same goal, make your Elasticsearch environment more secure.

We believe that the code of any security software has to be open by definition. All of our GitHub repositories, including the commercial modules, have always been open to the public. Customers can run their security audits on our code, and they can also compile it on their infrastructure. This is essential for any security-related software, and many of our customers do precisely that.

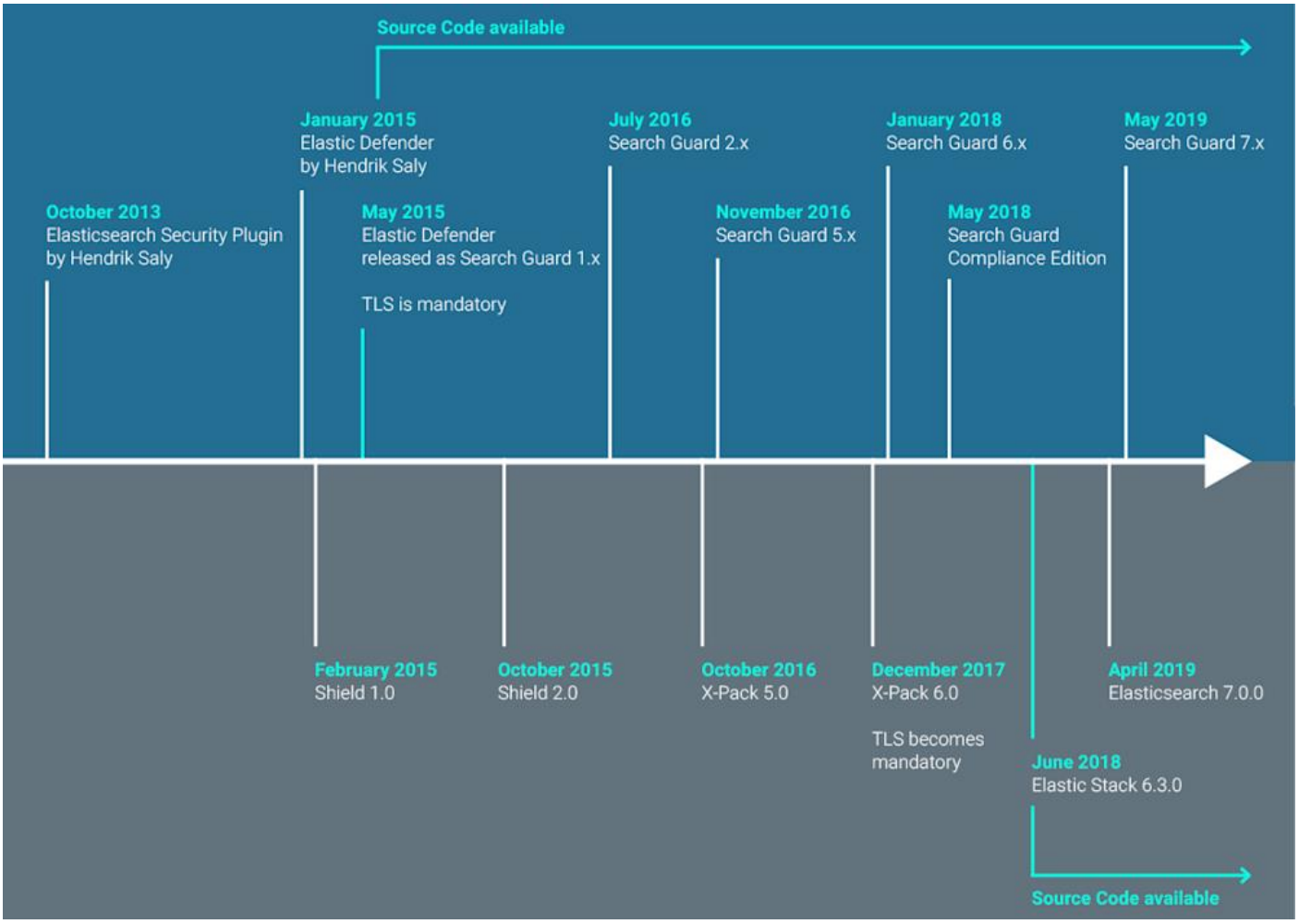
Veracode Verified

Search Guard also participates in CA Veracode Verified, a program that validates a company's secure software development processes. With approximately 30 percent of all breaches occurring as a result of a vulnerability at the application layer, software purchasers are demanding more insight into the security

of the software they are buying. CA Veracode Verified empowers us to demonstrate our commitment to creating secure software.

A paradigm shift

A lot has happened in the Elasticsearch ecosystem since the release of Search Guard 2.x, and a lot has changed for the better. Following our approach, TLS became mandatory for inter-node communication in 6.x, a fundamental principle that we drove forward since the first Search Guard release. In February 2018, Elastic finally decided to open their X-Pack code to the public. For the first time, users could inspect and review the X-Pack security code themselves before putting it into production. Again, a paradigm that we held high all the time.



Now Elastic finally announced they, too, will offer basic security features for free.

An "Elastic Stack Security Community Edition"

Elasticsearch announced that since version 6.8.x and 7.1.x, some security features are now free. The headline of the article is misleading because it implies that all of the Elastic Stack security features are now available free of charge. That is not the case. At closer look, the free Elastic security features include nearly the same features Search Guard always offered in the Community Edition at no cost. An *"Elastic Stack Security Community Edition"* so to speak. That was a long outstanding and necessary move for

Elastic. We very much appreciate and welcome these decisions, because they all help to increase the security for any Elasticsearch cluster.

The road ahead

For Search Guard, these moves verify our concepts and the decisions we made in the past. We will continue dedicating our passion for providing the best enterprise security solution for Elasticsearch available, and you can expect a lot of new and exciting features soon!

Jochen Kressin and the Search Guard team!

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-security-free-search-guard/