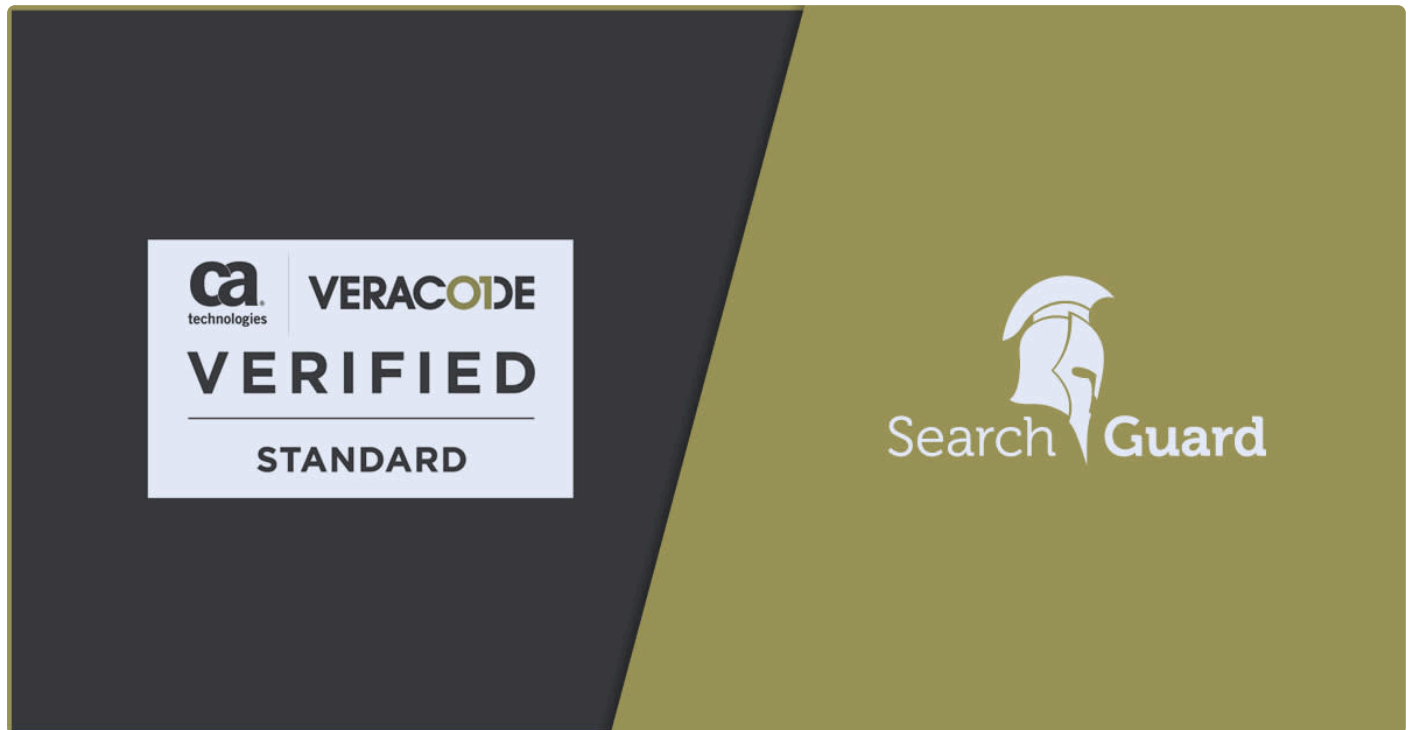


Search Guard achieves CA Veracode Verified Status

Jochen Kressin · 2018-05-19



Search Guard has always been Open Source. We made all of our source code available because we believe that [security software has to be Open Source](#) by definition: Everyone should have the possibility to inspect and audit our code before it is put in production. And many of our customers did precisely that. Today we are proud to announce that the security of Search Guard is now also officially verified by CA Veracode!

Search Guard 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:

<https://www.veracode.com/verified/directory> <https://www.veracode.com/ratings/floragunngmbh>

As part of CA Veracode Verified, we can now demonstrate through a seal and provide an attestation letter from an industry leader that Search Guard has undergone security testing as part of our development practice. Additionally, participating in the program ensures that our software meets a high standard of application security, reducing the risk for the customer.

By being accepted into the Veracode Verified Standard Tier, we have demonstrated that the following security gates have been implemented into our software development practice:

- Assesses first-party code with static analysis

- Documents that the application does not allow Very High flaws in first-party code
- Documents that there are no Very High flaws in third-party libraries we use
- Provides developers with remediation guidance when new defects are introduced

Quality Assurance at Search Guard

The Veracode Verified seal allows us to show that the Search Guard released and all used third-party libraries have been scanned for security vulnerabilities. But of course this is not enough to ensure consistent code quality, so we put a lot of time and energy into our quality processes.

Peer reviews

The first level of quality control is peer reviews. Any developer can request a review from a colleague at any time, and for critical changes in the core code of Search Guard these are mandatory.

Automated code reviews and analytics

We use [SonarQube](#) as the next line of defense against bugs and code smells. [SonarQube](#) is a platform to check code style, security, duplication, complexity and coverage of every change. It integrates with our build and release processes, so we can make sure every commit and pull request is checked. SonarQube also comes with plugins for all major IDEs so developers can detect and fix code flaws before they are even committed.

Unit Tests and continuous integration

Our Unit Tests are based on JUnit and test the Search Guard code both in isolation and also on a running Elasticsearch cluster. For testing the code on a running system, the tests spin up clusters of different sized and configurations in-process. The unit tests are executed for each commit and each Maven build. For continuous integration, we use [CircleCI](#) for its excellent support for Docker.

Integration Tests

While running tests in isolation or on an in-process Elasticsearch cluster help to find many nasty bugs and issues, they are not sufficient to provide Enterprise-grade software quality. Instead, you need to test the code extensively under real-world conditions. This is where our Docker-based integration tests come into play. Each test suite starts a test environment with dedicated Elasticsearch and Search Guard settings and also spins up services like LDAP, Kerberos, Keycloak or nginx. This makes it possible to test all features and different configurations on a real-world system. All editions and features of Search Guard are of course also tested on tribe nodes and with cross-cluster search. For testing the Kibana plugin, we use Selenium/Webdriver. The integration tests also run on CircleCI.

The integration tests not only help us to find and eliminate bugs and issues. While working on Search Guard 6 they were also able to detect issues in the beta versions of Elasticsearch. They were reported and fixed, and earned us the status as a member of the ElasticStack 6.0 Pioneer Program.

Performance Tests

The performance tests are executed on AWS and make sure that a new feature or change does not introduce any severe performance issues. It also allows us to benchmark a cluster with Search Guard installed against a vanilla Elasticsearch installation, or test the performance of various TLS settings and ciphers.

Security Scans

And now we're back at the beginning of this article. The security scans performed by the Veracode platform are integrated with our development and build processes so we can achieve consistent and regular scans of our code. The scans do not only include our own code but also check for vulnerabilities and issues in third-party library that we use and ship. As with SonarQube, Veracode also provides plugins for all major IDEs, which makes it convenient to examine the scan results and fix the code should there be any findings.

Summary

Achieving consistent, enterprise-level code quality and security is not an easy task. At Search Guard we go to great lengths to ensure the code we ship meets the very high standards for any security related software. Starting from peer reviews to unit- and integration tests to regular security scans we make sure that each release we ship is thoroughly tested from all angles. [Search Guard puts security first](#).

Where to go next

- Head over to GitHub and download and inspect the [code for Search Guard](#) and the [Enterprise modules](#)
- Follow our [documentation](#) for a [quickstart installation of Search Guard](#)
- Visit our [forum](#) in case you have any questions

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