Security means Open Source by definition

Claudia Kressin · 2017-10-26

Search Guard was and will always be Open Source software: The source code for both the Community Edition and the Enterprise Edition is available on GitHub, so everyone can download and inspect the complete code base. We decided to publish all of our code for one simple reason: You should never trust any security solution that is closed source!

> tl;dr: Security-related software has to be Open Source by definition. Since it is such a crucial and sensitive part of your infrastructure, you need to be able to inspect, audit and compile the code yourself. With closed source solutions, your only option is to just trust the vendor of the software.

What is Open Source?

This question seems to be a no-brainer, but in reality, people define the term Open Source differently. For us, it means that the source code of a piece of software is available for anyone to view and inspect. It does not necessarily mean that the product is available at no cost, and it does not mean that it is solely a community product. Open Source is not bound to a particular type of license. It can be published under MIT, GPL, Apache2, but also under a commercial license. But in all cases, you are able to inspect the code and compile the product yourself.

What is Closed Source?

Closed Source is the exact opposite: The source code of the software is not available for you to see. The product usually comes as a precompiled binary which you cannot inspect or modify. The only option you

have is to install it, and hope it does what it claims to do. And hope there are no security flaws or backdoors. And hope that security issues will be fixed promptly by the vendor. Many hopes for a crucial part of your infrastructure …

Why security software has to be Open Source

Cost of data breaches

The reason why any security-related software has to be Open Source is simple: You can't just trust the vendor! Security is a very sensitive topic, and the impact of a breach or stolen data can be devastating to your business. Not only can you lose the trust of your customers, leading to serious and negative effects on your revenue. If your infrastructure and processes need to be compliant with security regulations like HIPAA, SOX, PCI or GDPR, you can also face huge fines in case of breaches. For example, under GDPR "[o]rganizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million." (Source: http://www.eugdpr.org/gdpr-faqs.html).

While facing a fine for not complying with security regulations is one thing, losing the trust of your customers can shut down your business. Especially when you're storing sensitive information like personally identifiable information (PII), healthcare related or financial data. The OneLogin breach in 2017 clearly shows how damaging a loss in customer trust can be, and the IBM sponsored 2017 Cost of Data Breach study provides additional in-depth figures and statistics. Don't say you haven't been warned.

Source of data breaches – it's not always the malicious hacker

Some companies tend to be a bit sloppy on securing their data. One statement often is: "Our infrastructure is secured by a firewall already and runs in a trusted data center, plus we put a proxy in front of it. We're fine!" But studies have shown over and over again that one of the main threats to your data comes from the inside. Actually, external threats only account for less than half of the breaches. So, Insider threats outrank external attacks. Firewalls can be hacked and proxies can be circumvented. IP addresses and HTTP headers can be spoofed. And there's always the human factor as well. Somone might have misconfigured the firewall, set up some faulty iptables rules and suddenly your data is exposed without anyone noticing.

Security flaws are mostly unintended

While there's always a great fuzz about security software having some hidden backdoors you don't know about, the more dangerous issues are the unintended ones. Let's face it, no software will ever be free of bugs. So the big questions are:

- How can they be detected?
- How fast can they be detected?
- Who is able to detect them?
- How fast are they fixed?

A closed source solution is a black box. You don't know if there are any bugs, how severe they are, if they affect your specific use case and when they will be fixed. We believe this is not good enough when it comes to securing your data!

And don't just take our word for it

Luke J. McCormack, former Chief Information Officer of the Department of Homeland Security commented on the usage of Open Source security software:

> We believe moving towards Government-wide reuse of custom-developed code and releasing Federally-funded custom code as open source software has significant financial, technical, and cybersecurity benefits and will better enable DHS to meet our mission of securing the nation from the many threats we face.

(https://github.com/whitehouse/source-code-policy/issues/222)

Search Guard – The Open Source security suite for Elasticsearch

The code of Search Guard has always been Open Source, and we encourage anyone to inspect and review it before putting it in production. Search Guard already secures the sensitive data of major companies operating worldwide, including Fortune 500 enterprises. Our code has been audited several times by our customers or external companies tasked by our customers.

And if we claim that you should not simply trust your vendor, this of course also includes us. In contrast to using other, closed-source security solutions for Elasticsearch, with Search Guard you can run your own internal security audits. And by compiling the sources yourself, you can be 100% sure what exact code is running on your production environment to protect your valuable data, the foundation of your business.

Further readings:

- Search Guard main Git repository
- Search Guard official installation and configuration documentation

(Image: alexlms / shutterstock)

This article was published on the Search Guard blog: https://search-guard.com/blog/security-means-open-source-by-definition/