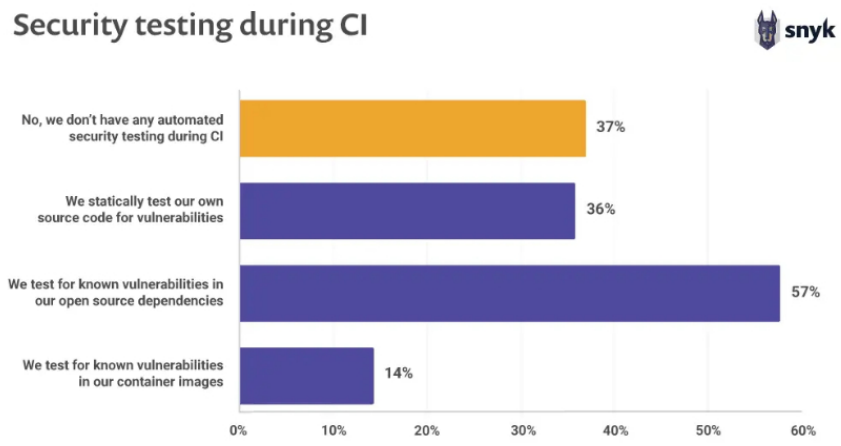
PCI standards open source security requirements — how to comply?

Written by: Rachel Cheyfitz Danny Grander

July 23, 2019 10 mins read

With the growing usage of open source security in the world of modern software development, there is an urgency to ensure open source is used in a secure way. However, open source security is not yet implemented across the board; a recent report conducted by Snyk found that 37% of open source developers don't implement any sort of security testing during their continuous integration (CI) process! The growth of open source alongside the lagging security standards has led many regulatory bodies and industry watchdogs to move toward stricter and clearer rules around how to protect applications that include open source code.



PCI picks up the open source mantle

In January of 2019, the Payment Card Industry Security Standards Council launched the PCI Software Security Framework (SSF), focused on application security. The Secure Software Lifecycle (SLC) Standard was also added—a subsection of the PCI Software Security Framework that outlines security requirements and assessment procedures for software vendors to validate how they manage security of payment software throughout the entire software lifecycle.

(Note: The new framework is replacing the current guidelines contained within the PCI Payment Application Data Security Standard [PCI PA-DSS], which will be retired in the coming years.)

At Snyk, we're happy to see PCI acknowledging the importance of securing open source components in the code and encouraging organizations to actively "shift left" in ownership of software development lifecyle security. The more we can incorporate security best practices early in the software lifecycle, especially when it comes to open source, the more secure our applications will be.

That said, as with lots of other compliance frameworks, it can be challenging to understand and implement new rules. So, we want to offer some insight into the new PCI compliance rules and share how to specifically comply with the open source-related aspects of the updated standard.

Who should care about the PCI updates?

The PCI Secure Software Standard (and the underlying SLC Standard) applies to payment software that is sold, distributed, or licensed to third parties for the purposes of carrying out payment transactions. Specifically, the PCI Software Security Framework is most relevant to vendors developing applications for payment processing and those selling those solutions to others. The update highlights that both security leadership and engineering teams must

selling those solutions to others. The update highlights that both security leadership and engineering teams must take responsibility for meeting compliance standards.

There are other rules that businesses who accept payments must concern themselves with under the PCI-DSS guidelines, but the standards we'll focus on in this post are directly relevant to the developers of the software.

No more one and done: The continuity key

Maybe the most important aspect of the new standard is the idea of **"continuous application security"**. The standard requires organizations to continuously monitor vulnerabilities and defenses, and requires them to adapt if the threat changes. Additionally, these organizations must continuously test application security controls and prove that their controls have not weakened or become ineffective over time. This is a high bar, and that's a good thing. It serves as a forcing function to treat security as part of the CI/CD process, rather than an afterthought.

What's behind the PCI updates? Why now?

So why exactly have these standards been updated? As we mentioned in our intro, software development has naturally evolved over the years, and the updated PCI standards are a thoughtful response to this evolution, updating the approach to software security in turn.Specifically, more and more software development strategies rely on open source components, so it was necessary to add requirements and controls that apply to open source. In our State of Open Source Security 2019 Report, we shared some statistics around the space, including these eye-openers:

- There has been an **88% increase** in application library vulnerabilities over two years**81% of respondents** believe developers should own security, but aren't well-equipped to do soOpen source maintainers want to be secure, but **70% lack skills**

In addition to the spread of open source development, many organizations now integrate security tools into the DevOps pipeline, and these security tools have gotten more proactive and effective over time. For this reason, it is both necessary and (the good news) more possible than ever to achieve robust security within **continuous development and integration cycles**.

The role of open source in the new PCI updates

Let's look in detail at the aspects of the new PCI rules that apply to open source software components. (You can also view the **standards** in full here.)

1. Security leaders' accountability

The text: Section 1.1 -- Accountability for ensuring the security of the vendor's products and services is formally assigned to an individual or team by the vendor's senior leadership.

What this means for you: Security leaders of large organizations must accept responsibility for security and make appropriate changes to development processes and tooling that will enable them to meet the updated PCI requirements.

How Snyk can help: Security leaders have plenty of priorities on their plates as it is. Snyk can streamline the process of meeting the new PCI standards by providing visibility into **open source dependencies and license risks** so that they can be addressed in a timely and appropriate manner.

2. The role of developers

The text: Section 1.2.a – Individuals (including third-party personnel) involved in the design, development, testing and maintenance of the vendor's products and services should be assigned responsibility and accountability for ensuring that its software is designed and maintained in accordance with its security strategy and all applicable security requirements.

What this means for you: The new requirements specifically call out the involvement and accountability of developers ("software-development personnel") to participate in the defined steps for meeting compliance.

How Snyk can help: Snyk's developer-first approach to security encourages developers to adopt security best practices easily. Snyk empowers developers to find and fix vulnerabilities as part of their existing software development process. Snyk also facilitates a one-click fix PR and fix automation process in the Git - in order to allow

developers to quickly address any vulnerabilities discovered.

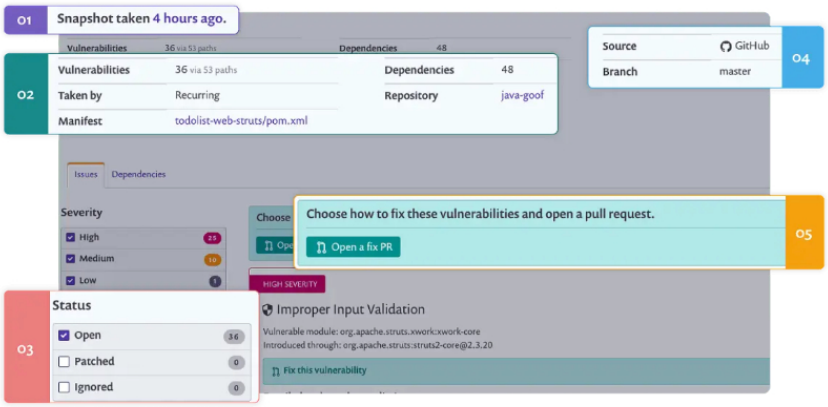
3. Open source components

The text: Section 3.2.b -- Where open-source software components are utilized as part of the software, the assessor shall examine vendor evidence, including process documentation and assessment results to confirm these components are managed.

What this means for you: Open source can be a huge boon in software development, but it's necessary to do your diligence before including any open source components in your application. The organization should:

- keep an inventory of all open-source components being used, including container images
- Develop a mature process to analyze and mitigate vulnerabilities
- Monitor vulnerabilities in open source components
- Implement a patching strategy

How Snyk can help: Snyk enables customers to map out dependencies in their applications, highlighting current vulnerabilities and continuously testing for new ones against a comprehensive vulnerability database. Snyk has a comprehensive patching and fixing capability with the automated fix pull requests that speed up triaging and fixing; essentially, Snyk automates the process of complying with 3.2.b, reducing manual efforts and thus time spent on compliance. With Snyk, teams can demonstrate that they have implemented checkpoints, remediation, and monitoring around potential vulnerabilities in open source components.

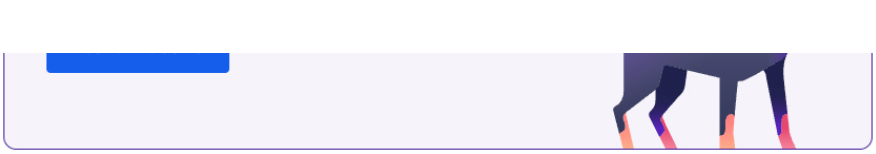


Using PCI compliance as a "shift left" motivator

As organizations continue to **shift left on security**, new challenges and opportunities arise. The updates to PCI compliance requirements make sense given the reality of today's software development processes and the pervasiveness of open source. While the requirements may seem steep at the outset, the reality is that meeting them will help your organization increase its security and reduce its overall risk profile, so it's an activity well worth the effort, even beyond the value of compliance.

The biggest challenge most organizations will face in meeting the new PCI standards will be to implement open source-specific security tools for the first time, since most do not have these in their arsenals. Incorporating open source security best practices into your CI/CD pipeline will make it a natural aspect of the development process, rather than a burden at the end or a scramble when new vulnerabilities are publicly disclosed.

To see how Snyk can help you meet the new **open source PCI compliance standards** with ease, developers can start using Snyk for free today.



Posted in: Compliance

snyk

The developer security platform

Snyk gives you the visibility, context, and control you need to work alongside developers on reducing application risk.

More about us