From License Compliance to Security:

Moonfare's Open Source Success Story

FOSSA

About Moonfare

- Manages more than $700+ million (€600+ million) for thousands of individual investors
- Headquartered in Germany with offices in Hong Kong and Luxembourg
- Earned the Wealth Management Innovation Award in the 2020 FinTech Breakthrough Awards program
- Recently joined forces with Fidelity International in a strategic partnership to broaden access to private asset investments

Moonfare is an EU-based fintech firm on a mission to make private equity more accessible to individual investors. Its web-based platform democratizes access to private equity markets.

“Private equity has traditionally been largely reserved for institutional and ultra-high net worth investors,” says Umut Koseali, Moonfare’s Head of Engineering. “Moonfare breaks down those minimums by applying technology so the company can scale up and down its operations really quickly without relying on manual labor.”

Like many of today’s most innovative companies, Moonfare uses open source software (OSS) to help power application development. Specifically, Moonfare leverages a number of JavaScript libraries that serve as foundational components in its best-in-class platform — a big reason why it’s grown from startup to global firm managing north of $700 million (€600 million) in assets in a few short years.

The company applies that same forward-thinking mentality to its open source vulnerability management and license compliance strategies. With an eye on further strengthening its compliance and security posture related to OSS, Moonfare implemented FOSSA, a software composition analysis (SCA) tool that automates and expedites key compliance and security workflows and processes.

Moonfare got up and running with FOSSA in just two days, enabling audit-grade reporting, continuous compliance with OSS licensing

requirements, and automated vulnerability identification and remediation.

> “FOSSA helped us tremendously in managing dependencies and compliance requirements. It is the golden standard for us.”
>
> **Umut Koseali,** Head of Engineering

Automating Open Source Security

The recent explosive growth in open source software usage has been accompanied by a significant spike in open source vulnerabilities. And when organizations don’t promptly identify and upgrade vulnerable versions of OSS packages, they leave themselves susceptible to attacks.

“There is a constant need for monitoring security patches and the newer versions in order to be secure and compliant,” Umut says.

Of course, there are several ways to go about doing this. Teams can manually track and implement available updates and patches, along with new CVEs. Or, they can automate the process.

FOSSA enables Moonfare to take the latter approach, strengthening security and making better use of staffing resources in the process.

> “Now that we’ve integrated FOSSA Software Composition Analysis with our codebase, we’re able to automatically update the packages whenever they have a newer version by creating automated change requests. This makes it easier for us to prioritize and remediate vulnerabilities.”
>
> **Umut Koseali,** Head of Engineering

Continuous Compliance

The open source software world is a vast and sometimes complicated one. There are countless libraries, hundreds of licenses, and a wide variety of compliance requirements. For example, a company might choose a certain library only to later realize that it’s pulled in dependency with a strong copyleft license.

“If you don’t pay attention to what you use in terms of licensing, you may end up being forced to open source your own code,” Umut says. “That’s something where everybody should be careful.”

Given the sheer volume of OSS components companies like Moonfare use, however, staying on top of every library and dependency — and ensuring engineering only uses licenses and libraries that the compliance team has greenlit — can be quite challenging.

FOSSA helps Moonfare overcome both of those challenges. It provides a complete inventory of Moonfare's OSS usage, including open source license types, direct and transitive dependencies, visibility into a variety of embedded, hidden, and declared OSS licenses in the source code, and more. Moonfare found these audit-grade reporting capabilities particularly valuable as it went through a recent due diligence process.

FOSSA also enables Moonfare's compliance team to easily apply policies that govern the company's use of open source. For example, FOSSA will fail a build if engineers pull licenses or libraries that conflict with Moonfare's policy settings.

"If you want to use a license, if you want to use a library, it has to fulfill the requirements of the compliance team," Umut says. "FOSSA helps us protect our intellectual property by applying those policies."

Efficient Open Source Management

FOSSA has helped Moonfare simplify and accelerate the process of meeting attribution requirements that come with certain OSS licenses. Instead of manually compiling all licenses and dependencies that go

into an attribution notice for a given project, Moonfare used FOSSA's reporting tool to publish a comprehensive attribution notices page to its website.

"We put everything in one place in order to attribute it to the authors," Umut says.

Given Moonfare's extensive use of open source and commitment to continuous compliance and security, Umut estimates FOSSA saves dozens of hours a month of team time on tasks related to open source management.

Couple these time savings with an improved security posture and audit-grade compliance — plus FOSSA's "super helpful" customer success team — and Moonfare remains a happy FOSSA user.

"Most of the time people create policies around compliance, but it's not easy to enforce those policies. Once you embrace FOSSA with the policy approach, then you can enforce any kind of policy around licensing by automating most of it," Umut says.

"Plus, from a vulnerability management standpoint, FOSSA creates automated change requests to our code to upgrade those packages, which speeds this process."

About FOSSA

Up to 90% of any piece of software is from open source, creating countless dependencies and areas of risk to manage. **FOSSA** is the most reliable automated policy engine for security management, license compliance, and code quality across the open source stack. With **FOSSA**, engineering, security, and legal teams all get complete and continuous risk mitigation for the entire software supply chain, integrated into each of their existing workflows. **FOSSA** enables organizations like Uber, Zendesk, Twitter, Verizon, Fitbit, and UiPath to manage their open source at scale and drive continuous innovation. Learn more at https://fossa.com.