MEND | adesso mobile solutions

adesso mobile Uses Mend to Secure Their Customers' Open Source Libraries

About adesso mobile

adesso mobile is a premium service provider for mobile businesses. For more than ten years, adesso mobile has been offering its customers the entire value chain from a single source. More than 250 employees work at 13 locations throughout Germany to develop individual solutions for and with customers. With cross platform expertise and distinctive industry know-how, adesso mobile provides customers with advice as a strategic partner already in the early phases of their projects.

adesso mobile supports its customers at every stage of a project – from initial analysis and consulting to development on all platforms and application management during operation. The modules of the service portfolio can be implemented as part of a comprehensive project or used as individual modules, depending on the requirements.

adesso mobile works with its own in-house teams as well as in joint project teams with customers. Regardless of the industry or the field of activity of the customers, adesso mobile develops concepts and solutions that are directly related to the core business processes.

The Challenge

adesso mobile has more than 100 customers worldwide, each with multiple projects under development. As part of certain contracts, adesso mobile provides customers with an inventory of the FOSS components used in the development of their mobile solution. Previously, this inventory was completed manually, a process that was inefficient and time consuming.

Can Özdemir, Head of Application Management at adesso mobile, knew there had to be a better way, so he began researching Software Composition Analysis (SCA) solutions to automate the process. “It didn’t make sense - and was no longer possible - to do this process manually,” says Özdemir.

adesso mobile had several unique challenges when considering an SCA solution. First, the company develops projects on a wide range of platforms from iOS to middleware to web front ends in almost every available language and uses a wide range of staging environments. Because of this, they required a solution with broad support for many different languages and package managers. Second, many of adesso mobile’s contracts stipulate that the company can’t move source code out of the EU or sometimes even out of Germany, where the company is based. Because of this, adesso mobile needed a solution that didn’t require direct access to source code or moving source code to the cloud to complete scans.

The Mend Solution

Based on their need for wide language coverage, adesso mobile considered both Mend Software and Black Duck when evaluating an SCA solution. adesso mobile ultimately selected Mend because it supported the many programming languages used by adesso mobile and was the only solution that didn’t require direct access to an application’s source code to complete scans.

Approximately 150 developers use Mend to scan their code on each commit. adesso mobile accesses Mend’s vulnerability and license compliance data via an API. Mend is integrated into the company’s TeamCity by JetBrains CI server.

At adesso mobile, every commit by a developer results in a build. Before the build, Mend scans each developer’s code for open source vulnerabilities and licensing compliance violations. When a scan is completed, results from Mend are generated as a job in TeamCity and delivered directly to developers. This means developers don’t have to leave their CI server to view results in a separate UI to resolve defects.

Once code is scanned, Mend produces reports on vulnerabilities and policy violations. adesso mobile uses Mend's policies to block open source libraries with security vulnerabilities or non-permissive licenses from entering their codebase. When a scan finds a vulnerable library or a non-permissive license, the build is failed and the artifact is not produced. adesso mobile's developers then use Mend to find a path to remediation that resolves the vulnerability or license issue.

adesso mobile finds that the impact of a vulnerability can be quite high with some open source libraries that have many dependencies, requiring both the platform lead and architect to conduct an in-depth analysis to determine the best way to remediate the vulnerability. "These vulnerabilities are so critical," says Özdemir, "that we may need to upgrade the whole component." When this occurs, Mend provides guidance and remediation advice so that the component can be safely upgraded without breaking the build.

The Results

Since implementing Mend, security has been shifted left. Developers are now able to scan their own code before a build. If a security vulnerability or restrictive license is found, developers can fix the defect before moving on to their next task. "Mend is straightforward for developers to use since it allows us to put clear policies in place," says Özdemir.

> *"As simple as it sounds - the Mend data is the biggest value add. The highest benefit for us is the detailed view of our software that Mend provides. When we deliver projects to our customers, we have confidence in knowing what open source it contains, which gives our customers confidence in us."*
>
> Can Özdemir, Head of Application Management at adesso mobile

Since adesso mobile implemented Mend to automatically scan open source components, the company has saved a lot of time remediating open source security vulnerabilities and license compliance issues. A manual process that took hours to review each application is now done in minutes. "It used to take us a minimum of five minutes to check an open source library, and each application has at least 10-20 libraries, not including dependencies," says Özdemir. "There are many more libraries to check when you add in dependencies."

With Mend, adesso mobile is able to automatically generate inventory reports on the open source components in their application's codebase. This makes it easier for adesso mobile's customers to approve the open source libraries contained in their application.

According to Özdemir, the best part of Mend is the visibility it gives adesso mobile into the open source in its codebase. "As simple as it sounds -- the Mend data is the biggest value add. The highest benefit for us is the detailed view of our software that Mend provides. When we deliver projects to our customers, we have confidence in knowing what open source it contains, which gives our customers confidence in us."