mend.io

Global Shipping and Mailing Company Uses Mend SCA and Mend SAST to Boost Product Security Affordably Across the SDLC

About The Company

A global shipping and mailing company that provides technology, logistics, and financial services to more than 90 percent of the Fortune 500. Small business, retail, enterprise, and government clients around the world rely on them to reduce the complexity of sending mail and parcels.

The Challenge

At this global shipping and mailing company, delivery is serious business – and so is building applications that ensure the timely delivery of packages and mail. Over 600 of the company's developers built applications using open source software components, and the company's product security team discovered a vulnerability that led to a reassessment of their security priorities.

"We found that our banking application had been compromised," said the company's Product Security Architect. "Our root cause analysis showed a vulnerable library, leading to the conclusion we needed to deploy an SCA [Software Composition Analysis] solution to understand our open source software use and how to best mitigate our risk."

In addition to seeking an SCA solution, the company also experienced challenges with its self-hosted SAST (Static Application Security Testing) solution, used to check for weaknesses in custom code.

According to the company's Product Security Architect: "The cost of hosting our previous solution, Checkmarx, became equal to the license itself. This is something we realized we couldn't sustain – even though the quality was there and it was a good tool, the hosting plus license cost was out of control."

Key Solution Requirements

SaaS Solution: The company sought out a solution that would give their product security team detailed scanning capabilities without the potential for rising hosting expenses. Ideally, the company hoped to keep proprietary code in-house, without needing to be stored by the scanning application, so that they could scan code belonging to vendors with an NDA in place.

Industry Trust: The company's product security team wanted no surprises and affordable renewals, so they turned to reviews on Gartner Peerspot and G2 to find solutions that were well-vetted by industry veterans, with transparent pricing and high user satisfaction.

Quality Technical Support: It was important to the company to have highly qualified support representatives available to answer questions. "On Mend's side, every support person is technical," said the company's Product Security Architect, noting that this is not true for all vendors in the space.

License Enforcement: In addition to detecting and remediating vulnerabilities, the company needed a solution capable of enforcing policies around open source software licenses, allowing them to automatically reject disallowed license types for improved license compliance.

The Mend.io Solution

Initially, the company started using Mend SCA for its 600 developers, then added Mend SAST to enable scans of both open source libraries and custom code. In addition to scanning using Mend's unified agent, the company has integrated scans into developers' IDEs and their build pipelines, allowing applications to be scanned at multiple development gates in the software development life cycle to ensure they meet quality and security requirements.

"The integrations mean that developers do not need to run a separate scan or use a separate application," the company's Product Security Architect explained. "They just use a browser extension, and then they know whether to download a particular library or not."

With the license policy enforcement capabilities offered by Mend SCA, he says, **"we can now bring the hammer down on license violations. Previously, we only focused on vulnerabilities, but our legal team was concerned about risk from license problems – now, developers can see what is violating policies and see a recommended alternative."**

The global shipping and mailing company has also begun using Mend for Containers in order to scan its container images for vulnerabilities and license violations. "We have a goal to unify our scans so that you can click on one module and see all three components – container scanning, SCA, and SAST findings, so that our teams can see three different reports and compare where they are to understand the security level of their product."

Solution Value & Benefits

As the global shipping and mailing company used the tools offered by Mend.io, the product security team noticed a significant unexpected side effect: developers were becoming far more informed and educated about vulnerable libraries and license policies.

"We've now reached a mature stage where developers know which libraries are vulnerable or not, even before they run the scan," said the company's Product Security Architect. "This is because of the education they receive from Mend's tools. When they used to run scans, they'd get 25 high severity vulnerabilities and 15 mediums. Now we get, at most, one or two high vulnerabilities, and they have a business case for the ones they have."

With over 600 developers relying on Mend.io scan results, support was important to the company. "From the day we adopted Mend SCA, support has been involved, and every support person is technical enough to answer our inquiries," he said.

The product security team also appreciates the significant savings Mend.io offers on infrastructure costs compared to its previous SAST solution, as well as the value represented by having multiple solutions included with the SCA offering. "Not all solutions offer container scanning and license policy enforcement," he added. "With Mend.io, you have the license aspect and the cloud native aspect and it's all in the existing license model, without additional costs."

About mend.io

Mend.io, formerly known as WhiteSource, effortlessly secures what developers create. Mend.io uniquely removes the burden of application security, allowing development teams to deliver quality, secure code, faster. With a proven track record of successfully meeting complex and large-scale application security needs, the world's most demanding software developers rely on Mend.io. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, the open- source automated dependency update project.

For more information, visit www.mend.io, the Mend.io blog, and Mend.io on LinkedIn and Twitter.