mend.io

Mend.io Empowers OM1

to Ensure Software Quality and Regulatory Compliance Standards

About OM1

OM1 is re-imagining real-world data and evidence by developing large, electronically-connected networks of health data in immunology, cardiometabolic, mental health, neuroscience, respiratory, and ENT specialty areas.

Leveraging its extensive clinical networks, unparalleled technology, and industry-leading artificial intelligence platform, OM1 offers enriched healthcare datasets, advanced platforms for regulatory-compliant real-world studies, and personalized medicine solutions. With a focus on deep clinical insights, the offerings are used to unlock the power of healthcare data to measure and predict outcomes, accelerate medical research, and improve clinical decision making.

The Challenge

OM1 collects medical data from many sources, including Electronic Medical Records (EMR) systems, health claims from doctors and hospitals, and even directly from patients and their medical devices. In addition to data collection, OM1 develops applications that consume and analyze that data.

To develop those apps securely, they needed more visibility. VP Product Engineering Neil Davies said: **"We were completely in the dark as to what sorts of vulnerabilities we had, as well as their impact. It was a big gap we had to address in our app stack – and we also needed to understand where we were with open source licensing."**

Key Solution Requirements

Combined license and vulnerability management: OM1 wanted a unified solution that could help them with vulnerabilities and licensing risk, rather than paying for separate solutions.

Compliance reporting: During a funding round, OM1 had to use manual, time-consuming processes to conduct due diligence around their open source risk. They needed to simplify and accelerate due diligence and SOC2 reporting, and ensure they could demonstrate HIPAA compliance.

Block bad builds: OM1 had tried using Dependabot to manage out-of-date dependencies, but it gave them no way to stop a build that violated policies. They wanted a solution that could be set up to block any build with high severity vulnerabilities or disallowed license types.

Highly configurable: OM1 wanted to avoid "click ops." "I wanted everything configurable through code, so we could manage it through code," said Davies.

The Mend.io Solution

OM1 set up Mend SCA by using a Terraform provider to configure SCA scanning as code, then built a container to do all the scanning in their Jenkins build pipeline. Once the deployment began, the vulnerabilities and license violation notifications started coming in.

"First, we had to slowly work through channels to make sure everything got fixed, to the point where we no longer had any high-severity vulnerabilities," said Davies. **"Once we had that in place, we turned on the blocking of high and critical vulnerabilities – if you had one, it would fail your build, and it would need to be resolved in order to pass, or you would need to document an exception in the code and have it approved."**

In addition to using vulnerability and license detection from Mend SCA to ensure quality builds, Davies said OM1 has also found value in the Mend Renovate capabilities included in Mend SCA, which make it easy to find and update out-of-date open source components.

"We're trying to roll out more use of the Renovate application to track not just vulnerabilities, but also how up-to-date our libraries are. Our goal is to get to 85% up-to-date libraries across all of our applications and services," Davies said.

For developers at OM1, adjusting to Mend SCA scanning was made easier due to its built-in capabilities for creating pull requests. “People have adjusted to the new process and realized it’s not as painful as it seems,” said Davies. **“We’ve got Mend Renovate pushing out those PRs (pull requests) for people, and it does a much better job than Dependabot – we’ve gotten PRs from Dependabot that just don’t work, and then the Mend PRs do.”**

Solution Value & Benefits

For OM1, compliance – and being able to prove that compliance to stakeholders – has been the key value of Mend SCA.

“We wanted a solution that would make doing due diligence trivial – and the Mend SCA solution did that very well,” Davies said. “We can also now demonstrate that we meet our HIPAA requirements.”

These assurances have, in turn, led to an easier path to business growth for OM1. “Knowing we have these tools in place is huge, because we can now answer security questions from customers,” Davies explained. “If you can’t answer those questions, it’s a big problem for trying to close deals – but we can show what we do, and we have had no issues with anyone complaining about our vulnerability program.”

The configurability of Mend SCA has enabled OM1 to implement high standards for software builds: vulnerabilities close to 0 (barring documented exceptions) and at least 85% of open source libraries up-to-date.

OM1 plans to drive even more value from Mend SCA by implementing longitudinal tracking to understand vulnerability trends over time. Davies considers Mend SCA an indispensable tool: **“If we stopped using Mend SCA, we’d be putting the company at risk from software vulnerabilities – and we wouldn’t get deals to close, because we couldn’t meet our compliance requirements.”**

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, link here, 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.