



Global Media and Technology Company
Chooses Mend to Mitigate Open Source
Security Risks

About Global Media

This publicly traded, US-based global media and technology company is valued at more than \$200B and is one of the largest broadcasting and cable television providers in the world. With almost 200,000 employees, this company is also one of the largest internet and telephone service providers in the US.

The Challenge

As a result of a number of high-profile security breaches including Equifax's 2017 data breach, this global media company wanted to be more proactive in its approach to application security to prevent both risk to its large customer base as well as the damage a potential breach would cause to its trusted brand. Though the media company's security has always been world class at the network layer, the company needed to focus on the application layer.

From a technical perspective, the media company has a highly diverse development environment with a wide array of platforms and languages. "The diversity you see in the wild roughly mirrors the diversity you see inside our company," says their senior director of DevSecOps transformation. Prior to Mend, development teams within the media company performed ad hoc pen testing, but they knew they needed a more robust approach. To achieve the best results, the media company decided to integrate security into the development process and have developers buy into security much earlier in the SDLC.

The DevSecOps team is responsible for coaching developers on how to use best-of-breed tools to create more secure code.

"The role of my organization is to get development teams to take a bigger ownership interest in the security of their products, so we are only integrating tools into their pipeline. We don't maintain our own pipeline," says the senior director of DevSecOps transformation.

Open source vulnerabilities were a huge concern for the media company throughout this process. In certain stacks, it's not uncommon for 80% or more of the company's code to be made up of open source components. The remaining code written in house is primarily to stitch together the open source functionality. One of the company's main requirements was to give its developers a tool to secure and manage its extensive open source code.

The Mend Solution

After a competitive evaluation, the media company chose Mend. One of Mend's key differentiators is its comprehensive coverage and broad support of more than 200 programming languages. "One of the things we like about Mend is it covers every platform we use. Mend supports pretty much every possible stack," says the senior director of DevSecOps transformation.

Another key differentiator is Mend Prioritize. Prioritize scans open source components with known vulnerabilities to assess whether proprietary code is making calls to vulnerable methods. This reduces false positives and allows the media company to focus on real vulnerabilities in their open source code. "Mend telling us whether we're using the vulnerability is still pretty killer, and we're starting to use Mend Prioritize more and more," says the senior director of DevSecOps transformation.

In addition, because so much of the media company's code is open source, the company needed a solution that put open source software security first. Mend ensures that no open source component or dependency is overlooked, providing faster development without compromising security.



“We really want teams to take ownership of the security function, so we bake it into their pipeline. Once a team decides they are going to gate developers’ commits through checks like Mend, security posture goes way up. That is the furthest left we can shift.”

Another goal of the DevSecOps transformation team was to shift application security left. To do so, the media company integrated Mend into its CI/CD pipeline.

“We really want teams to take ownership of the security function, so we bake it into their pipeline. Once a team decides they are going to gate developers’ commits through checks like Mend, security posture goes way up. That is the furthest left we can shift.”

The Results

Mend has helped the media company bring order and security to its open source usage. The media company says Mend is more reliable than the competitors, easier to integrate, and less expensive on a per-developer basis. Ease of use is particularly important. If a security tool doesn’t easily integrate with other developer tools, developers won’t use it.

Mend also allows the media company to be more efficient by giving significantly lower false positives when identifying vulnerabilities. By matching reported vulnerabilities to open source libraries, Mend Prioritize is able to determine whether the media company’s open source code actually uses a known vulnerability. This reduces false-positive security alerts by up to 85% and allows the media company to focus on critical issues first.

The mission of the DevSecOps team is to focus on the bigger security picture, which includes establishing better security practices and processes for the entire organization. The media company is able to achieve this by transitioning most of the day-to-day security work into developers’ hands. Mend is one of the tools that makes this possible.

As open source usage grows, the media company continues to need robust tools that enhance the security and development of its own offerings. “Mend is literally our only dedicated offering in the Software Composition Analysis space. It is the first tool we talk about.” Using Mend helps this large media organization mitigate a bigger security risk.

About Mend

Mend, formerly known as WhiteSource, effortlessly secures what developers create. Mend 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. 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.

Related Resources

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