MEND | Trimble

Case Study - Trimble Uses Mend to Monitor Open Source Globally

Trimble's 3,000 developers use Mend to identify and remediate vulnerable open source libraries.

About Trimble

Trimble is an industrial technology company transforming the way the world works by delivering solutions that enable its customers to thrive. Core technologies in positioning, modeling, connectivity and data analytics connect the digital and physical worlds to improve productivity, quality, safety, transparency and sustainability. From purpose-built products to enterprise lifecycle solutions, Trimble is transforming industries such as agriculture, construction, geospatial, and transportation. Founded in 1978, Trimble is a publicly traded company (TRMB) valued at USD 22.4B and is based in Sunnyvale, California with employees in more than 40 countries worldwide.

The Challenge

In 2017, Trimble started looking for a solution that would give the company visibility into its open source use. The main goals were to better understand and assess the licensing compliance and security risk of the open source components used in the company's commercial products, including their SaaS platforms, on-premises software, and hardware devices. After a thorough evaluation, Trimble chose Mend.

About a year ago, Trimble initiated a global company-wide cybersecurity initiative. "We had a flurry of activity across the entire company to operationalize our cybersecurity process," says Nick Banta, Vice President of Global Cybersecurity at Trimble. "Understanding threats and vulnerabilities are key to delivering viable products. There are many avenues that need to be assessed to have a fully mature security process. We got to the point in our evolution where open source software analysis was where we needed to focus to increase our overall maturity."

Trimble required a solution that the company could query programmatically to gain full visibility into their open source use. They also needed a tool that would allow developers to take ownership over their open source use to develop securely. Fortunately, Trimble already had Mend in place being used by many developers, so the company decided to roll it out worldwide.

The Mend Solution

Mend allows Trimble to improve their overall security posture. "Our development teams are focused on our SaaS application space to continually identify and manage security vulnerabilities. Mend is a major contributor to that function," says Banta. "We use the data Mend generates by looking at code repositories to track and manage our open source security risk. These metrics show the cybersecurity health of our different products."

Not only does Mend give Trimble's security team valuable data about their open source risk, but it also allows developers to code more securely. "The security team can get access to all this great information in Mend and pull it into our shared metrics platform. Developers can also fully operate it on their own to prevent vulnerable libraries from entering their code base. Having one tool that could be used by both teams was a natural synergy for us."

Banta says that Mend has been really easy for developers to adopt. "We find that developers prefer to have the tools to manage their own security during development. Mend allows them to fix issues in their code repository by clicking a button. The metrics go down to zero immediately so they can handle it all on their own." Giving developers the tools to code securely frees up the security team to focus on more challenging work such as the prioritization and remediation of other security vulnerabilities. The ease of use for developers combined with the programmatic access to data allows Trimble to drive value from Mend. This represents the realization of the shift left mentality.

The Results

"Mend allows us to unlock the ability to manage and remediate the risk that is in our product. This would be virtually impossible to do without Mend," says Banta. "We're now in a continual operational process where we can track development life cycles and show where the vulnerabilities pop up within libraries and see those get patched on a 30-, 60-, or 90-day scale. We're at a point where scanning has become just a part of the process. Mend makes it easy because we can enumerate all of the different libraries and repositories, and tie them back to our products." Trimble uses Mend to prioritize vulnerabilities based both on the criticality of the application as well as severity using CVSS scores to remediate the most critical issues first.

> *"This helps us understand the developer community and think about what other kinds of tools we could use that would be a natural fit for the different languages we use. It allows us to have better conversations around horizontal services. Knowing what languages you use helps you provide the right developer tools."*
>
> Nick Banta, Vice President of Global Cybersecurity

"Mend allows us to unlock the ability to manage and remediate the risk that is in our product. This would be virtually impossible to do without Mend," says Banta. "We're now in a continual operational process where we can track development life cycles and show where the vulnerabilities pop up within libraries and see those get patched on a 30-, 60-, or 90-day scale. We're at a point where scanning has become just a part of the process. Mend makes it easy because we can enumerate all of the different libraries and repositories, and tie them back to our products." Trimble uses Mend to prioritize vulnerabilities based both on the criticality of the application as well as severity using CVSS scores to remediate the most critical issues first.

In addition to application security, Trimble uses Mend in several other ways:

• **Acquisitions.** Trimble uses Mend to gauge the health of potential acquisitions. "When we acquire a software or hardware company, we use Mend as part of our due diligence process to understand what we're buying," says Banta. "If we can see a lot of open source libraries that haven't been patched or updated, that's an indicator of the amount of tech debt in the product that we're considering purchasing and integrating into our product suite."

• **Collaboration.** An unexpected benefit of using Mend is its analytics allows Banta and his team to identify the most popular open source libraries throughout the company. A handful of open source libraries are used persistently in thousands of repositories. Trimble connects developers across the globe who are using these high-frequency libraries so that they can collaborate and share knowledge about how to best leverage and secure these libraries. "Mend allows our developers to work together to utilize core library functionality in a more efficient manner, which is a value add."

• **Language support.** Because Mend supports more than 200 programming languages, Trimble is able to use Mend analytics to identify which languages are most popular throughout the company. "This helps us understand the developer community and think about what other kinds of tools we could use that would be a natural fit for the different languages we use. It allows us to have better conversations around horizontal services. Knowing what languages you use helps you provide the right developer tools," says Banta.

Trimble performs around 30,000 Mend scans each month and has remediated more than 330,000 alerts in the past 12 months. The recent adoption of Mend's developer integrations, which allow vulnerabilities to be remediated earlier in development, has been well received by developers.

When asked about return on investment, Banta says, "It is hard to assign a value to an incident you prevented from happening. You need to understand and manage your risks. Your company and customers demand it. You can not put a price on trust, and Mend helps us maintain the trust we have with our customers."

About Mend

Mend helps organizations accelerate the development of secure software at scale. We provide automated tools that bridge the security knowledge gap, integrating easily into the software development life cycle and going beyond detection with a remediation-first approach. Mend is built on the most comprehensive vulnerability database in the industry, providing the widest coverage for threats and attack vectors. Our solution helps enterprises reduce risk and increase the productivity of their security and development teams. For more information, visit www.Mend.io

Related Resources

Learn more at www.mend.io