MEND | **NSI** Northern Safety & Industrial

Northern Safety & Industrial Secures eCommerce Site Using Mend

About Northern Safety & Industrial

Based in Utica, NY, Northern Safety & Industrial is a subsidiary of the German Würth Group, valued at 14.27 billion EUR. Through their website, Northern Safety & Industrial sells a range of protective and emergency gear for business clients in a diverse range of sectors including construction, agriculture, food services, medical, and more. Northern Safety & Industrial has more than 1,000 employees, which includes an in-house development team that is responsible for the company's eCommerce platform and internal applications.

The Challenge

Northern Safety & Industrial decided to adopt an open source management platform in part to achieve their goal of being PCI DSS compliant. The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

As a retailer that processes payments online, the company knew that protecting their customers' private information was essential for their business. To this end, they needed to implement a solution that would scan their open source components for vulnerabilities without taking up a lot of their developers' time.

"Our documentation says to check for updates for any open source components once a quarter, but even that wasn't realistic," says Jeremy Bailey, Applications Development Manager at Northern Safety & Industrial. The policy was designed to look at only sources that formed the major project that comprises their code, but manually checking for updates for even this limited scope was an onerous and time-consuming task. According to Bailey, manually updating all the projects his team was working on, including the 30 or so plugins, JavaScript code, and dependencies was outside his team's capacity.

The time and effort needed to sort through the information on each component to find the right update meant that updating their open source code was nearly impossible.

Northern Safety & Industrial makes a point of working according to best practices. Bailey cites how seriously his team takes OWASP's Top 10 warning against using components with known vulnerabilities. "Understanding which open source libraries you're using and knowing if there are any security vulnerabilities is extremely important to us," says Bailey.

Simply put, Bailey and Northern Safety & Industrial needed a tool that would automatically detect vulnerable open source components and help them to remediate vulnerabilities quickly, allowing their developers to focus on developing.

> *What I like about Mend is that it runs in the background and therefore doesn't disrupt the developer's workflow. They can develop, but at the same time, as a manager, I am aware of any potential issues and have them resolved before it becomes too costly.*

The Mend Solution

Northern Safety & Industrial installed Mend's SaaS product into their Azure DevOps environment and was up and running in a matter of minutes. "I did not want to have to do a lot of heavy installation, configuration, and maintenance, so I loved how Mend was set up as a service," says Bailey. "And the fact that it just worked was one of the key selling points for us."

Through Mend's integration with Azure DevOps, Northern Safety & Industrial doesn't have to leave Microsoft's platform to ensure that their software is secure from open source vulnerabilities. If Northern Safety & Industrial wants to view all components in every product or project, they can go to the Mend dashboard to access a full report of their open source component inventory.

Mend also helps Northern Safety & Industrial's developers code more securely without adding additional development time. "What I like about Mend is that it runs in the background and therefore doesn't disrupt the developer's workflow. They can develop, but at the same time, as a manager, I can become aware of any potential issues and have them resolved," says Bailey.

One of Northern Safety & Industrial's favorite features is Mend's policies. The Mend platform enables security and compliance professionals to enforce policies automatically throughout the software development life cycle. Policies define a set of rules that reflect how an organization handles specific conditions, such as high-security vulnerabilities, when they are detected in the open source components used by its software.

When configuring Mend, Northern Safety & Industrial created policies on open source component use that reflected their security and legal standards. If a developer tries to use an open source component that violates these policies — for example if a component was found to have a known vulnerability — that component is blocked from entering their codebase, even going so far as to fail the build if a non-compliant piece of code is identified.

If a policy violation occurs, the appropriate managers are notified to follow up with information about the offending component. Since policies are in place to block any libraries that do not meet Northern Safety & Industrial's standards, the company doesn't have to worry about introducing vulnerabilities or unwanted licenses into their build.

> *Mend is a part of our safety net in that it alleviates developers from having to be constantly reviewing vulnerability issues. Developers can just develop, rather than worry about vulnerabilities and licenses. In terms of ROI, Mend pays for itself.*

The Results

Northern Safety & Industrial relies on Mend to deliver a full range of essential services for open source security and license management. Mend is able to help Northern Safety & Industrial prevent components with high risk vulnerabilities from being brought into their codebase, making their overall solution more secure for their customers.

Constantly running in the background, Mend is continuously updating the company's database to identify new vulnerabilities from multiple sources beyond what is produced by the National Vulnerabilities Database (NVD), sending alerts for necessary patches. Bailey notes how his team is currently working on patching a vulnerability that Mend had pointed to in a specific project where they were using Angular.js, explaining that since they use

the versions that were identified as high impact on their public facing eCommerce page, it saved them from a potential XSS attack.

Along with QA and code reviews, Mend is an integral part of Northern Safety & Industrial's security process.

"Mend is a part of our safety net in that it alleviates developers from having to be constantly reviewing vulnerability issues or always checking out the latest version of the Angular platform codes to see if there's a new vulnerability that started," says Bailey. "They can just develop, rather than having to worry about vulnerabilities and licenses."

Mend has been a valuable investment for Northern Safety & Industrial, saving many hours of developers' time. "I was able to bring Mend to my boss as a ROI and told him, look, this pays for itself," says Bailey.

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.