



Case Study - Microsoft uses Mend
for open source security

About Microsoft

Microsoft is one of the world's best known corporations. They produce computer software, consumer electronics, personal computers, and related services such as cloud services. Microsoft employs 181,000 people worldwide, including about 85,000 software developers.

The Challenge

Microsoft developers use a lot of open source software — over 80,000 distinct open source packages are used over 11 million times in Microsoft's entire code base.

To help Microsoft's 85,000 developers be confident in their use of open source software, the Microsoft 1ES team — which selects and manages all the tools that Microsoft developers use — was tasked with finding the best open source software security tool. They wanted a tool that was extremely accurate, easy to use, and provided actionable recommendations for how to fix vulnerable open source packages.

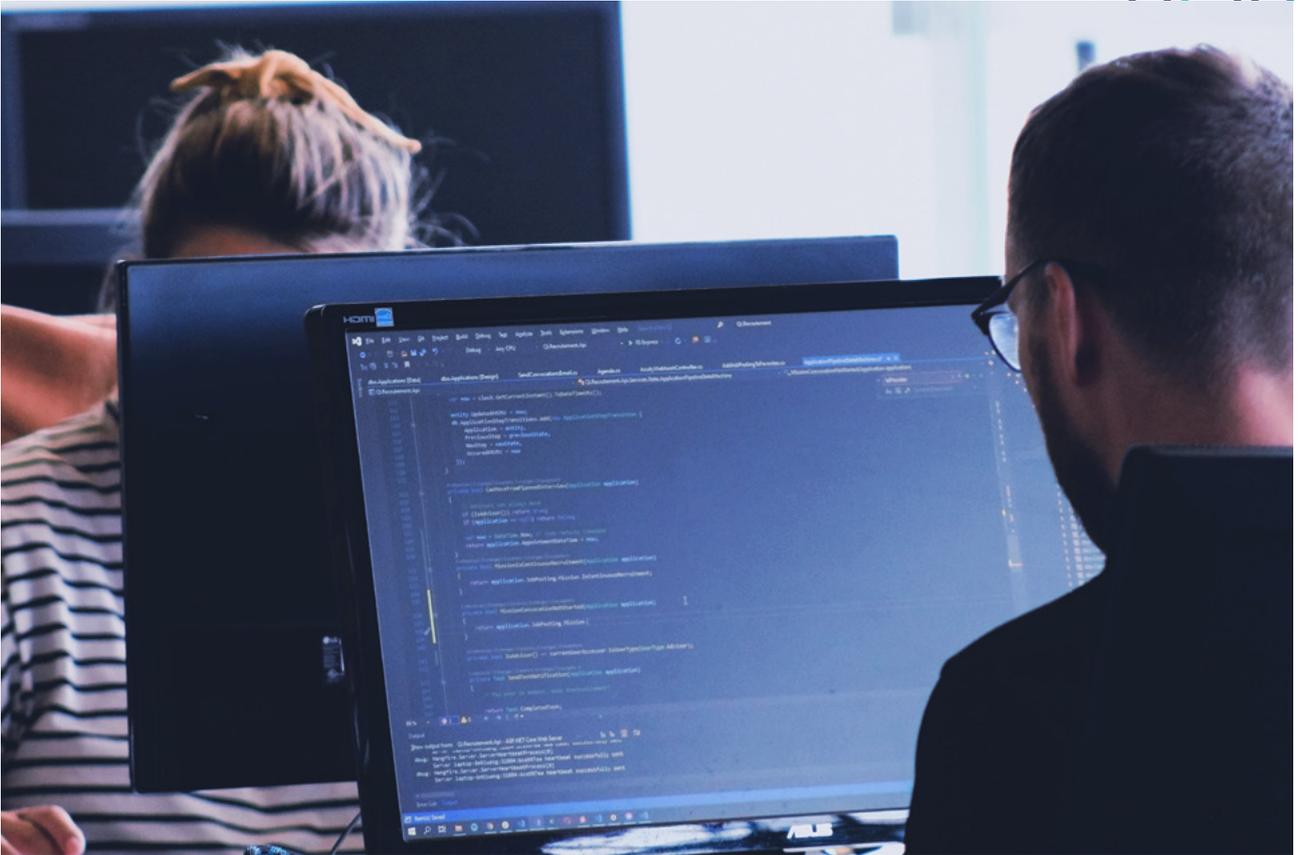
The Mend Solution

Microsoft chose Mend for several reasons:

- **High accuracy.** According to Magnus Hedlund, the Director of Engineering for the 1ES team at Microsoft: "The easiest way to lose a developer's trust is to give them a false positive. If you give false positive results, developers will tune out that tool and not look at it again. Microsoft relies on Mend to give high quality recommendations with very low false positive rates."
- **Ease of use.** Magnus Hedlund again: "We integrate Mend vulnerability detection directly into the developer's workflow. Without developers doing anything, we automatically scan for vulnerabilities and notify them of their vulnerable code."
- **Great remediation advice.** "Identifying the vulnerabilities and telling developers they have a problem is useful, but if you don't tell them how to fix it, they can't make it better. Without the remediation recommendation there is no point raising a number of alerts that nobody can do anything about. The detailed remediation advice provided by Mend enables Microsoft engineers to quickly upgrade their packages to less vulnerable versions."



It was very important for us to partner with a company that was keeping up to the mark in terms of the new trends in the industry, making sure that their data was accurate. But then also one of the most important aspects that we had was the data that we are getting needed to be actionable. We needed to have the right set of recommendations



The Results

Bryan Sullivan, manager of Microsoft's 1ES security tooling group said: "Mend plays an integral part in helping us identify where we're using potentially risky or insecure open source and getting that addressed as early as possible. We rely on Mend for great remediation guidance. Remediation guidance is extremely critical to helping developers fix the problem correctly the first time, every time."

Poonam Gupta, the Director of Microsoft's 1ES team said: "Working with Mend has been the right decision. When we have the right set of recommendations, we feel more secure. Mend has been able to scale to our needs. It's been able to scale to the ecosystems that we want to cover. Overall it's been a great decision."

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, [link here](#), the open-source automated dependency update project.

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