mend.io | SEAGATE

Seagate Uses Mend Repository Integrations to Gain Full Visibility Over Open Source

About

Seagate Technology crafts the datasphere, helping to maximize humanity's potential by innovating world-class, precision-engineered data storage and management solutions with a focus on sustainable partnerships. A global technology leader for more than 40 years, the company has shipped over four billion terabytes of data capacity.

The Challenge

Seagate began as a hard disk drive (HDD) manufacturer producing products for many years with closed-source code. In recent years, they expanded their product offerings to include a broader roadmap of data storage products utilizing cloud-based services and Open-Source Software (OSS). As the company launched these new types of products and services with OSS, their Product Security Office (PSO) needed to mobilize a centralized Software Composition Analysis (SCA) Application Security (AppSec) program to service the many Seagate teams now using OSS.

Seagate has benefited from many acquisitions and expanding product lines, which has brought a wide variety of technology stacks to Seagate. This makes securing OSS a particularly complex endeavor, with different product teams using different technology stacks. To ensure the solution was making a difference, they needed visibility over all product lines – plus benchmarking to get a handle on whether their code was getting more or less secure over time.

Key Solution Requirements

- **Repo Integrations:** Teams at Seagate use various repositories, including Bitbucket, GitLab and GitHub. To keep their open source components secure at scale, they need a product that can integrate seamlessly with all of them, so developers can continue to use the tools they are accustomed to.
- **Full visibility:** Seagate's PSO needs the ability to see security trends for the company overall and within individual product lines, to better understand which part of their business needs improvement.
- **Policy enforcement:** Seagate needs to enforce policies around open-source vulnerabilities and licensing, with enough granularity to create different policy sets for specific application contexts.
- **Due diligence reporting:** The legal teams at Seagate need a solution to automate the creation of standard due diligence reports, as well as notify developers and team leads.

The Mend Solution

Seagate requires a tool that will lay over the top of their decentralized and diverse landscape. Seagate regards Mend SCA as the best tool to achieve broad OSS security coverage across all their repositories and CI/CD pipelines, while also maintaining central visibility and control over policies across multiple business units.

Mend's seamless repository integrations – including Bitbucket, GitLab and GitHub – allows Seagate's teams to secure their OSS without leaving their repo of choice. Mend's highly configurable SCA solution ensures that Seagate's highly varied teams can scan in the ways that make sense for their unique situations: some use repo integrations to scan continuously, while other product teams use automated or manual pipeline scanning.

Expanding the deployment after an initial successful rollout was complicated and time-consuming. Seagate relied on Mend support for help along the way. "It's been a highly cooperative scale-up," said a spokesperson from Seagate's PSO. "Since we've started working with Mend, we've grown tremendously in terms of the number of licenses and libraries. And as we've grown, Mend has grown with us- highly cooperative and very engaged."

Seagate's PSO gained visibility over the entire organization and within product lines, using Mend's holistic executive reporting. "Mend helps us with our benchmarking by telling us the overall customer average for percent of vulnerable libraries and the percent of vulnerability that are severe," said Seagate's PSO. "We communicate those benchmark metrics alongside our performance and hold ourselves accountable to exceed the watermark of those metrics."

While the legal team was impressed by Mend's built-in automated due diligence reporting, their process of notifying developer teams remained highly manual. Mend's support teams learned about these processes and recommended a new tactic: using Mend's JIRA ticketing integration to automatically create tickets assigned to a developer.

Solution Value & Benefits

"The biggest value that we get out of Mend is broad visibility into our open-source usage across the company," said Seagate's PSO. "We partner with the development teams that utilize this tool and they have many different libraries and software stacks." Using Mend, Seagate allows developers to continue using libraries in the way that makes the most sense to them – but with increased risk management and improved visibility to the organization.

Seagate's PSO said security teams at Seagate particularly appreciate Mend's reporting tools: "Knowing what libraries we use at the corporate level is essential. Mend also lets us see licensing and dependencies. When it comes to using different versions of packages, Mend makes it easy to know what needs to be updated, and what is from multiple versions ago."

Seagate's PSO reports key security metrics for each product line visible to the entire organization. According to Seagate's PSO, a "competitive spirit" has developed as a result, with teams challenging one another to drive metric improvements.

Seagate continues to find new ways to maximize solution value from Mend, adding product teams that start using open source, expanding JIRA ticketing for license policy violations to the entire organization, and continuing to encourage integrated and automated scanning.

"For us, that's why Mend is imperative. Mend had the wherewithal to engage with us and listen to our feedback, then come to us with things we could implement and improve together. Mend's support enabled a great relationship to form and mature. Today, we're feeling the benefits of the partnership that has led to increased success at Seagate."

About mend.io

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