CASE STUDY:

SaaS Company’s Transformation with Seal Security

The Backdrop

A rapidly growing SaaS company with a team of 75 software developers, quickly making its mark in the tech world, was accompanied by a significant challenge: numerous critical open source vulnerabilities that posed a serious risk to the progress of the company. With 200 critical vulnerabilities identified, half of which were unique, the company's resources were stretched thin, consuming 5% of the developers' capacity to address these issues. The developers were being sidetracked by complex framework issues that were extremely time-consuming to address.

A Security Bottleneck

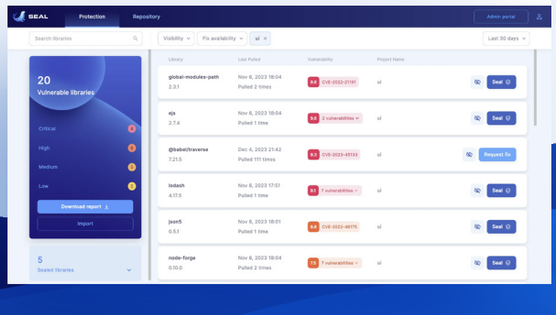
The company's security team, comprised of only two people, was too small to effectively manage the list of vulnerabilities. This shifted the weight onto the developers, who were already tasked with driving the company's innovation forward. The additional load of patching and major code changes led to internal friction and a chaotic environment, as most developers lacked the expertise in updating code and managing dependencies without risking breaking changes.

Customer Confidence at Risk

The stakes were high, as customers, requiring assurance of robust security for their sensitive information, started to express doubts. Prospects demanded vulnerability scans before finalizing contracts, and the company often found itself failing these evaluations, leading to lost business opportunities and delayed sales cycles.

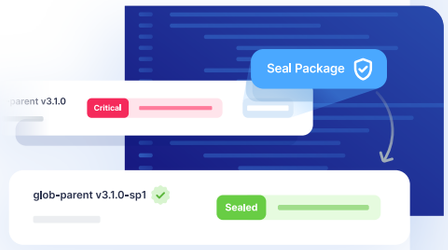
The Turning Point with Seal Security

The partnership with Seal Security marked a new chapter for the SaaS company. First, Seal Security synchronized with the company’s source code repository. By configuring Seal to serve as the primary artifact server, they created a centralized hub for all software builds and dependencies. This strategic move allowed the company to seamlessly access and deploy all the remediated packages, ensuring that each component was up to date and secure.



The Transformation

- Seal Security enhanced code security by offering standalone security patches for 99% of all critical vulnerabilities and provided organizations with centralized control over the vulnerability patching process.
- Compliance with industry standards, including FedRAMP was now within reach, reassuring prospects, and customers alike.
- The company successfully managed customer Service Level Agreements (SLAs), confidently passing all product security scans. This allowed them to guarantee their prospects and customers that the software provided was free from vulnerabilities.
- The security team was empowered with tools and capabilities to handle vulnerabilities independently, without relying on the development team.
- The Mean Time to Repair (MTTR) was significantly reduced from months to hours, minimizing downtime and improving productivity.
- Cost savings were realized as technical debt was reduced, and developers could refocus on feature development and technological advancements.



The Conclusion

With Seal Security's solutions, the SaaS company successfully navigated its most pressing challenges. Developers returned to their primary roles, driving growth through innovation, while the security team confidently managed the vulnerabilities, ensuring compliance and customer trust. The company emerged not just unscathed but stronger, with a robust security posture that promised a secure and promising future.

About Seal Security

Seal Security is the first AI solution for automated, scalable open source vulnerability remediation. This technology provides organizations with centralized control over the vulnerability patching process, eliminating the need for R&D team involvement. Offering standalone security patches in six programming languages, Seal Security ensures seamless and predictable remediation of vulnerabilities in direct and transitive dependencies, regardless of public maintainers' involvement. This enables security teams to respond immediately, reducing Mean Time to Repair (MTTR) from weeks to hours and significantly decreasing manual effort and technical debt.

For more information contact: info@sealsecurity.io