

Case study

Kitework's Strategic Response to CentOS End-of-Life with Seal Security

The Backdrop

Kiteworks, a California-based technology company, secures sensitive content communications across various channels, including email, file sharing, file transfer, managed file transfer, web forms, and APIs. They faced a significant challenge when Red Hat announced that support for CentOS images would end in June 2024. With some third-party libraries already lacking security updates, Kiteworks' systems were left vulnerable, accumulating dozens of critical vulnerabilities without a viable solution.

A Security Bottleneck

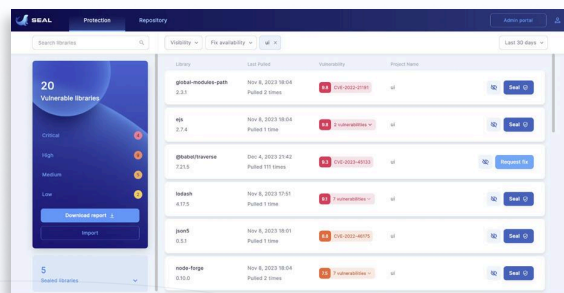
Maintaining FedRAMP compliance was crucial for Kiteworks, which became difficult as support was withdrawn by Red Hat, leaving numerous vulnerabilities unaddressed. Although Kiteworks employed a solution and used a prioritization tool, these measures only identified problems without offering solutions. The only viable option seemed to be migrating to a different Linux distribution - a process that would take more than 6 months with the risk of breaking changes.

Customer Confidence at Risk

The loss of support heightened customer concerns about security, as many had strict federal requirements regarding vulnerability risk. Kiteworks was spending significant resources to meet these requirements, finding themselves stuck in an endless cycle of putting out fires to maintain compliance.

The Turning Point with Seal Security

Partnering with Seal Security marked a significant turnaround. Seal Security integrated with Kiteworks' source code repository and became part of their software build process, enabling centralized governance and patching capabilities. In their next deployment cycle, the customers' vulnerability requirements were successfully fulfilled for the first time without Kiteworks having to spend time on remediation. This has allowed Kiteworks to plan a more managed migration to a new Linux system without immediate pressure or fear of breaking changes, while maintaining FedRAMP compliance.



The Transformation

Kiteworks' partnership with Seal Security proved transformative, enabling them to patch all CentOS-related vulnerabilities swiftly, thus maintaining FedRAMP compliance and mitigating immediate security risks. This strategic response not only allowed Kiteworks to pass critical vulnerability scans, securing customer trust and business continuity, but also provided the flexibility to plan and test a migration to an alternative Linux distribution without the risk of disruptive changes.



The Conclusion

With Seal Security's innovative solutions, Kiteworks successfully navigated the challenges posed by the CentOS EOL. The development team could focus on innovation and growth, while the security team managed vulnerabilities confidently, ensuring compliance and maintaining customer trust. Kiteworks not only emerged unscathed but also strengthened, with a robust security posture ensuring a secure 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.

