CASE STUDY

# Replicated Speeds Up CVE Patches and Reclaims Engineering Resources with Chainguard

Replicated, a leading provider of cloud-native application tools and solutions, offers a platform to help software vendors distribute commercial applications to their own customers' self-managed Kubernetes environments. Replicated helps vendors build better releases, install apps and updates faster, support efficiently, and measure what matters. Given this important role, protecting vendors and their customers from CVEs is a critical part of secure software delivery and management. To address this challenge and enhance security for their customers, Replicated partnered with Chainguard Images to reduce CVEs in third-party open source libraries.

## Challenge

Vulnerability sprawl is the rate at which CVEs accumulate in software or popular container images and applications and how quickly engineering teams are able to realistically update and mitigate known CVEs in a required or expected period of time. Our research found popular container images, when not updated, accumulate one known vulnerability per day. This doesn't account for the countless false positives that are also being flagged daily to engineering teams by the scanners they use.

When you combine the reality of vulnerability sprawl and the high rate of false positives, you end up with a lot of time spent mitigating risk when you could be building or innovating the next project.

Replicated recognized the importance of maintaining a secure and robust environment for their vendors' applications running on Kubernetes. Because Replicated and its vendors leverage a wide range of open source and proprietary tools, it became clear there was a need to proactively address CVEs and enhance the processes to mitigate them. Replicated's engineering team were spending precious time and resources patching and triaging CVEs to keep vendor environments for their customers secure. The team needed a solution to help cut down this time spent patching vulnerabilities, but one that also presented an opportunity to use only hardened images with secure-by-default capabilities.

**To alleviate these concerns and proactively address potential security risks in its software, Replicated sought a solution that would help mitigate CVEs at the source. This led to their adoption of Chainguard Images.**

Chainguard Images offered a more efficient solution to address the time spent patching CVEs, and will help Replicated to more quickly triage any future vulnerabilities from false positives.

Chainguard REPLICATED

By addressing the vulnerabilities at the earliest stage of the image creation process, Chainguard Images will significantly reduce the chance of CVEs impacting Replicated's software vendor customers who are using the Replicated platform to provide products and solutions to their own customers. This proactive approach by Replicated to adopt Chainguard Images provided added assurance to Replicated's software vendors and their own enterprise customers, enabling them to deploy and manage their applications on Kubernetes with greater confidence in image security and hygiene. Additionally, with the extra time spent not patching low severity CVEs, Replicated's engineering team was able to focus on other software supply chain security priorities like Software Bill of Materials (SBOMs), software provenance and Vulnerability Exploitability eXchange (VEX).

### One Solution for Platform and Security Teams

Selling an engineering team on a security solution is not as easy as it may seem. As a company rooted in engineering, at Chainguard we know what it is like when we hear about a new security tool or solution that is going to help us be more secure without hindering our workflow. There is often a hesitation and frustration that yet another step is going to be added that may impact our productivity. We expected to run into this exact scenario when we started talking to companies about Chainguard and our products. With Replicated, we had proven our value to the security team by showing them how we could solve their vulnerability sprawl problem, but faced some hesitation from the platform engineering team that using our base images wouldn't hinder their day-to-day work.

> **We have a new project our engineers are working on that uses Go. Our engineering staff setup the docker file to use the Docker Hub Golang image. I took a look at the image, and it has 66 reported vulnerabilities whereas the Chainguard Golang image has zero. It took me about 20 minutes and 6 lines of code to change it over to use the Chainguard Image. There is no blame to engineering, they are doing what everyone does by just taking what's in Docker Hub."**
>
> **– ANDREW STORMS, REPLICATED CISO**

Working hand in hand with Replicated's platform engineering team to quell these concerns, Chainguard was able to address the team's feedback and prove that we weren't going to be another security tool that gets in their way. Instead, we enhanced this foundational engineering work by offering a solution in our Chainguard Images that is both secure and designed with a developer-first mindset based on the tools they know and love. As a team of builders, our mission is to give other builders the tools they need to do their jobs right from the start.

## Chainguard Images Delivers Success for Replicated

Replicated's collaboration with Chainguard Images proved to be instrumental in enhancing the security and reliability of the Replicated platform. By mitigating the CVEs associated with external dependencies, Chainguard Images played a pivotal role in ensuring that Replicated's customers could operate their applications in Kubernetes environments with minimal security risks.

> **In May 2023, in our KOTS repo, we bumped versions of third party software 568 times due to vulnerabilities. I'm certain there were lower severity vulnerabilities that just didn't get addressed because it wasn't worth the effort to go after every vulnerability. This morning, I saw our latest KOTS Chainguard Image and found zero vulnerabilities."**
>
> **– ANDREW STORMS, REPLICATED CISO**

The proactive approach adopted by Chainguard Images aligned perfectly with Replicated's commitment to delivering robust and trustworthy solutions. By addressing vulnerabilities at the source, Replicated could reduce its attack surface, offering customers peace of mind and an increased level of confidence in their deployment processes.

Furthermore, the partnership with Chainguard Images enabled Replicated to maintain a strong reputation as a provider of secure and reliable cloud-native application management tools.

As the industry continues to evolve, Replicated's investment in proactively managing CVEs through their partnership with Chainguard Images positions them as a trusted partner for software vendors and enterprises alike. The enhanced security measures contribute to the overall stability and resilience of vendors' applications running on Kubernetes clusters.

---

## Ready to lock down your supply chain?

Talk to our customer obsessed, community-driven team.

contact@chainguard.dev