Chainguard | ANDURIL

Anduril trusts Chainguard to innovate at mission speed and scale

About Anduril

Anduril operates at the forefront of AI-powered defense solutions, developing unmanned systems such as drones and submarines to protect the lives of Americans serving on the frontline. These mission-critical solutions depend on the secure, reliable, and rapid deployment of proprietary software.

> **We're different from a commercial tech company, mainly because we get targeted on a regular basis by nation state actors. And because of that, we have to think about security a little bit differently.**
>
> JOE MCCAFFREY, CISO, ANDURIL

To meet the highest standards of security and reliability, Anduril turned to Chainguard to help protect its software supply chain. Every container image Anduril uses had to be free of known vulnerabilities and ready for rapid deployment, powering mission-critical defense systems without slowing innovation.

The challenge

Before Chainguard, Anduril was locked in a never-ending cycle of vulnerability triage to maintain a zero-CVE mandate. Meeting strict Department of War and customer security requirements meant patching CVEs across a rapidly growing estate of container images. This effort would have required building and sustaining a sizable team dedicated to image hardening and remediation – both for the upfront work and ongoing maintenance.

Joe McCaffrey, Anduril's CISO explained, "Our ability to meet DoW and customer security requirements was very difficult because we had to patch CVEs at scale. And with the amount of software that we build, doing that across all of our container images is nearly impossible, or it would've required us to build and maintain a large team to do that. And that was not something that we were interested in doing."

Anduril's hypergrowth compounded the challenge. As Amanda Huey, Software Engineer at Anduril, explained, "Because we grew so fast and our business lines increased so rapidly, a lot of open source code was being brought in that wasn't checked for vulnerabilities beforehand. That just continued to create technical debt on our end of remediation and patching."

What felt manageable with a handful of deployments became untenable at scale: engineering time dedicated to product development bled into vulnerability work, slowing feature delivery and sapping momentum. JP Ratliff, Software Engineering Manager at Anduril explained, "It was such a heavy load on the engineering team that we couldn't ship new features." The team needed a partner that could make secure, zero-CVE containers the default so developers could get back to shipping mission-critical capabilities.

> **Prior to Chainguard, we were really chasing our tail when it came to vulnerability management and maintaining the zero-CVE posture.**
>
> JOE MCCAFFREY, CISO, ANDURIL

The solution

Recognizing the burden and risks associated with their home-grown image pipeline, Anduril turned to Chainguard Containers to do the heavy lifting. The time-to-value for Anduril was immense.

As Amanda explained, "To get up and running with Chainguard was actually really easy. We were able to just utilize the documentation provided. It took about a day to set up and we were able to utilize Chainguard images quickly."

> **It was probably one of the easiest integrations that we've ever done with third-party software. Basically, we just would drop in the Chainguard Container—rebuild the deployment, ship, test, ship. And that was it."**
>
> JP RATLIFF, SOFTWARE ENGINEERING MANAGER, ANDURIL

The results

Partnering with Chainguard delivered transformative results across Anduril's security and engineering teams, reshaping both operations and culture.

Scaling secure software with speed

With trusted open source from Chainguard, Anduril's application security and platform teams dramatically reduced engineering toil. Time previously spent on CVE remediation, ATO processes, and triaging customer scan results was reclaimed, allowing engineers to focus on platform innovation and advanced defense technology, rather than maintaining bespoke image pipelines.

"My life has changed drastically since adopting Chainguard. I've been able to focus more on feature development and designing new features for Anduril rather than vulnerability patching," Amanda shared.

> **Now that we've implemented Chainguard, our developers no longer have to worry about the patching of the underlying base image, and they can focus on doing what they do best, which is building software.**
>
> JOE MCCAFFREY, CISO, ANDURIL

The culture around open source has shifted as well. JP explained, "Before Chainguard, we were very cautious about bringing in new open source containers because you just don't know what you're going to get. Now if it's covered under the Chainguard umbrella, we just bring it in. We don't need to worry about it, it's great."

The build-vs-buy verdict

The takeaway was clear. Trying to stand up what JP referred to as an internal "software factory" would have burned countless engineering hours for marginal gain. Chainguard has already built what we call the Chainguard Factory. Standing up this kind of secure software pipeline internally is notoriously difficult, but with the Chainguard Factory, companies like Anduril don't have to reinvent the wheel, enabling them to focus on mission-critical innovation instead of vulnerability triage.

As JP summed it up: "Don't do it yourself. Don't even think about it. You are going to lose so many engineering hours trying to build a software factory to handle this when it already exists with Chainguard."