At Chainguard, we hold ourselves to the highest standards of security, but as a start up, unlimited resources to devote to certifications like SOC 2 are unrealistic. However, we saw a unique opportunity to practice what we preach by using our own product for our SOC 2 certification — Chainguard Images, which cut common vulnerabilities and exposures (CVEs) on average by 97.6%. By dogfooding (i.e. using our own technology in the process) in this way, SOC 2 requirements were easier to meet, helping ease the burden of the certification process.

Challenge
Founded in 2021, Chainguard is both a startup and a group of seasoned security veterans keen to pursue the best ideas in open source security. Since our inception, SOC 2 compliance has been extremely important to our business growth and maturity. More than a security certification, SOC 2 is an indicator of trustworthiness, because a SOC 2-compliant organization is secure in both its data and business practices. Companies must carefully consider and demonstrate their dedication to maintaining a strong security position over an extended period. Whereas working with non-compliant companies is increasingly seen as a risk, becoming compliant not only positions us as more reliable partners in terms of information security and compliance, but also demonstrates our holistic commitment to best practices when it comes to all things cybersecurity.

But preparing for a SOC 2 audit is a lot of work, and being Type II certified requires tracking and addressing all the company's vulnerabilities over a six-month period. This meant tracking access to company systems, vulnerabilities we saw, and how we addressed those vulnerabilities.
Vulnerability management is a huge source of toil in security engineering. As a one-person team, I can’t look at thousands of vulnerabilities and do everything else in my job. I’m lucky that I use our own products like Chainguard Images. Because we have so few CVEs in our production fleet, the vulnerability management part of my role takes so little time.”

— THOMAS STRÖMBERG, DIRECTOR OF SECURITY AT CHAINGUARD

Solution

Chainguard Images drastically reduce vulnerabilities in open source software and shrink container image attack surface by nearly 80% thanks to three guiding principles.

1. Chainguard Images are designed to be minimal, containing only what is required to build or run an application and its runtime dependencies. This means that developers only need to focus on fixing the vulnerabilities that an application explicitly uses.
2. We engage in reproducible builds, making it easier to track changes from one build to the next.
3. Chainguard Images are always up-to-date because Chainguard rebuilds them every night — unlike slower iteration cycles that can produce vulnerability creep for users.

Because Chainguard Images are always built on the most recent, secure software, there are very few recent vulnerabilities to address on any given day, which smoothed the way for SOC 2 certification. Not only do our customers trust Chainguard products because Chainguard is now SOC 2 certified, but using Chainguard solutions will lighten the lift for our customers’ SOC 2 certification processes, too, by minimizing the time, effort, and resources that would otherwise be sunk into vulnerability management.

You can download and view and download Chainguard’s SOC 2 certification here.