Chainguard | Canva

Canva trusts Chainguard to eliminate supply chain risk for its platform serving 260 million monthly users

About Canva

Launched in 2013, Canva is an online design and publishing tool with a mission to empower everyone in the world to design anything and publish anywhere.

Canva runs one of the largest and fastest-moving engineering organizations in Australia, with around 3,000 engineers building and deploying software leveraged by 260 million monthly users across the world. As a cloud-native company, almost everything Canva ships runs in containers, and the sheer breadth of what the team builds means the company relies heavily on open source at every layer of the stack.

The challenge

When your engineering organization spans thousands of developers pulling container images from public registries, vulnerability management becomes a structural problem. Canva was inheriting constant CVEs baked into the base OS layer of upstream images, many of which had nothing to do with software its engineers actually wrote.

"It was a constant treadmill that mainly fell on the shoulders of our security and platform teams," said Adam Mills, Senior Engineering Manager at Canva. "Security toil creates friction. Our platform teams wanted to give developers a fast, safe path to production."

New CVEs were disclosed every week, upstream images updated on their own schedules, and the burden of keeping everything current was pulling engineering time away from higher-value work. As Canva grew, so did the volume of vulnerabilities to manage. The math stopped working: you cannot linearly scale security headcount to match engineering growth.

But assessing risk didn't stop at container images. As Adam explained, "Containers came first, because the blast radius is obvious and the tooling to detect CVEs there is mature, so you feel the pain acutely. But libraries, in particular, Python, represent a different and arguably more insidious risk. A malicious package can sit quietly in your dependency tree for a long time before anyone notices. In some ways, that's a much scarier threat model."

Security controls were reactive rather than preventive, checking to see if Canva was safe from a malware attack after it was released to public registries rather than systematically eliminating risk at the source.

The solution

Canva evaluated several approaches, including building a solution internally. Angus Lees, Principal Software Engineer at Canva, explained why the team chose Chainguard instead:

> "With Chainguard, we get minimalism combined with verifiable proof of trust through signed SBOMs and provenance.
>
> Angus Lees, Principal Software Engineer, Canva

For containers, the must-have criteria included proven CVE reduction at scale, a credible SLA for remediation of critical CVEs, and a broad enough container image catalog to cover Canva's workloads. For libraries, the requirement was simpler: drop-in compatibility. Canva could not layer in new security controls that slowed down its team of 3,000 engineers. The ability to use Chainguard Libraries without disrupting the current developer experience was non-negotiable.

Chainguard Libraries went into production within a few weeks of access, with no rewrites needed. "That kind of low-friction adoption matters a lot when you're trying to roll something out across a large engineering organization," said Adam.

> "The ability to proxy through Chainguard Libraries without disrupting developer experience was non-negotiable.
>
> Adam Mills, Senior Engineering Manager, Canva

The results

Invisible quality improvement

The best outcome is the one engineers don't notice, and that's what Canva achieved in adopting Chainguard. Engineers pull a Chainguard Container; it works, and they don't get hit with a wall of CVE alerts from the base OS.

"We want our platform to be the easiest and safest path to production, and Chainguard is a big part of making that true," said Adam.

A stronger supply chain security posture

Chainguard Libraries address the supply chain attack surface in Canva's Python ecosystem in a way that is transparent to developers.

"Our risk profile and exposure to that ecosystem has changed significantly," Angus said. "We now know that those libraries are a clean room built from a secure source. From a platform perspective, we give that freedom to our developers where they can pick the libraries they need, and at the same time we know that we're getting the secure result we need."

Together, Chainguard Containers and Libraries dramatically shrink the attack surface across both infrastructure and application layers, extending a consistent philosophy: start from a trusted source.

Security maturity as a competitive advantage

Canva serves 260 million monthly users and a growing number of enterprise customers with significant security requirements. A transparent supply chain security posture, backed by hardened container images, verified provenance, continuous CVE remediation, and a preventative approach to malicious libraries, is how Canva demonstrates security maturity to customers. As Angus explained, "For Canva, security is no longer a nice to have. It's now a competitive requirement."