Chainguard | elastic

Elastic trusts Chainguard to harden the foundation its entire artifact portfolio ships on

Elastic is the company behind the Elasticsearch Platform, serving tens of thousands of organizations with search, observability, and security solutions, including in highly regulated environments. Open source is core to Elastic's ethos: Elasticsearch itself is open source, and its broader stack relies heavily on open source components. That's both a strength and a continuous responsibility.

The challenge

At Elastic's scale, container security is an operational discipline. With thousands of engineers globally and an open-source-rooted artifact portfolio, keeping every image free of known vulnerabilities was a growing burden, and Elastic's push toward FedRAMP High accreditation raised the stakes further.

Three challenges converged: CVE remediation was consuming significant platform engineering capacity; FIPS-validated cryptographic modules, required for regulated environments, were costly to maintain in-house; and vulnerability work kept slipping to the final stages of the release cycle, repeatedly delaying Elastic Stack releases.

As Maha Alsayasneh, Senior Engineering Manager at Elastic, put it: "We were spending too much time on the back foot. Every release cycle, we'd find ourselves chasing CVEs into the final days before GA. That's not a sustainable place to operate when you're shipping at our scale and into our regulatory environments."

Building and maintaining a hardened, FIPS-validated image foundation in-house proved structurally untenable. It would require a dedicated team plus significant investment just to stand up FIPS-validated builds. The consequences were real: commercial customers faced slower access to new features, and public sector customers hit a hard barrier. FedRAMP High wasn't accessible without solving this properly.

The solution

When Elastic ran the build-vs-buy math honestly, the answer was clear. Elastic turned to Chainguard Containers as the base layer for its published artifacts.

Rather than standing up an internal hardened image factory, Elastic recognized that Chainguard had already built one with the Chainguard Factory, continuous CVE remediation built in, and FIPS-validated variants included.

The integration fit cleanly into Elastic's existing infrastructure: Chainguard Containers flow through its Buildkite-based CI and ArgoCD-driven GitOps workflows, are scanned by Snyk, validated by automated quality gates, and ship to downstream registries without disruption.

> “ The moment we ran our first Chainguard-based image through our pipeline and saw the scan results come back clean, we knew this was the right decision.
>
> Maha Alsayasneh, Senior Engineering Manager, Elastic

The results

Engineering capacity reclaimed

The most immediate impact was felt by the Platform Engineering Productivity team responsible for the frameworks, tooling, and infrastructure that allow all of Elastic's product teams to build and release at scale. CVE toil dropped significantly, and the capacity previously absorbed by image hardening work was redirected toward platform innovation.

Product teams saw fewer late-cycle CVE scrambles disrupting their delivery plans, and Release Engineering gained a more predictable release cadence with CVE compliance built into the base layer rather than patched in at the end.

FedRAMP High unlocked

The ability to point to hardened, FIPS-validated, continuously updated container images removed a hard blocker on Elastic's path to regulated markets. For security and compliance teams, it created a stronger, audit-ready baseline. For public sector customers, it meant Elastic could now credibly compete for and serve accounts where supply chain integrity is a real procurement criterion, markets that simply weren't accessible before.

Increased speed and confidence

Perhaps the most durable change inspired by bringing on Chainguard was cultural. Before Chainguard, every new open source dependency triggered a security review and a remediation plan. Now, if it's available through the Chainguard Repository, it's already trusted. As Maha described it, the team has shifted "from a defensive posture to a confident one," building with confidence rather than caution. And for Maha, the broader lesson is one any engineering leader will recognize: supply chain security isn't a problem you solve once and walk away from. It's a continuous discipline—the question is whether you staff for it internally or outsource to a dedicated partner.

> “ If you're operating in regulated environments and considering whether to build this internally, my honest advice is don't. The depth of what Chainguard has built — and continues to build — would take years and a serious team to replicate. Partner with them and put your engineers on the work only your company can do.
>
> Maha Alsayasneh, Senior Engineering Manager, Elastic